

THE ALGEBRAIC THEORY OF VALUED FIELDS

MICHEL KOSTERS

ABSTRACT. In this exposition we discuss the theory of algebraic extensions of valued fields. Our approach is mostly through Galois theory. Most of the results are well-known, but some are new. No previous knowledge on the theory of valuations is needed.

CONTENTS

1. Introduction	1
2. Definition of valuations	2
3. Main results	3
3.1. Properties of extensions of valuations	3
3.2. Normal extensions	4
3.3. Algebraic extensions	7
4. Preliminaries	10
4.1. Field theory	10
4.2. Tate's lemma	13
4.3. Ordered abelian groups	14
5. Extending valuations	15
6. Normal extensions	17
6.1. Finite normal extensions	17
6.2. Normal extensions	20
7. Algebraic extensions	23
7.1. Proofs	23
7.2. Finding extensions explicitly	28
8. Defects in the discrete case	29
References	31

1. INTRODUCTION

General valuation theory plays an important role in many areas in mathematics. Also in this thesis, we will quite often need valuation theory, although for our applications the theory of discrete valuations suffices. There exist many books on valuation theory, such as [End72], [EP05], [Kuh] and [Efr06]. They do not treat the case of algebraic extensions of valuations theory completely. Furthermore,

Date: April 16, 2014.

2010 *Mathematics Subject Classification.* 13A18, 12J20, 12J10.

This article is part of my PhD thesis written under the supervision of Hendrik Lenstra. I would like to congratulate him with his 65th birthday and as a present give him the reference he subtly requested.

definitions of certain concepts are not uniform. This article is written to fill this gap in the literature and provide a useful reference, even when restricting to the case of discrete valuations. Our definitions are motivated by our Galois theoretic approach. No previous knowledge on the theory of valuations is needed and only a slight proficiency in commutative algebra suffices (see for example [AM69] and [Lan02]).

With this in mind, this article starts with definitions and the main statements. In the second part of this article we will provide complete proofs. In the last part of this article we give examples of extensions with a defect.

Our treatment of valuation theory starts with normal extensions of valued fields. Later, by looking at group actions on fundamental sets, we prove statements for algebraic extensions of valued fields. The beginning of our Galois-theoretic approach follows parts of [End72] and [EP05], although we prove that certain actions are transitive in a different way. The upcoming book [Kuh] uses at certain points a very similar approach.

Even though most of the statements in this article are known, there are a couple of new contributions.

- We define when algebraic extensions of valued fields are *immediate*, *unramified*, *tame*, *local*, *totally ramified* or *totally wild* (Definition 3.2). The definitions are motivated by practicality coming from Galois theory. We also study maximal respectively minimal extensions with these properties (Theorem 3.15).
- We compute several quantities, such as separable residue field degree extension, tame ramification index and more in finite algebraic extensions of valued fields in terms of automorphism groups (Proposition 3.7). We will give necessary and sufficient conditions for algebraic extensions of valued fields to be immediate, unramified, ... in terms of automorphism groups and fundamental sets (Theorem 3.10). Current literature only seems to handle the Galois case.
- Another notable result is Theorem 3.8: classical sequences from valuation theory split if a specific residue field has some properties.

For a field K we denote by \overline{K} an algebraic closure. For a domain R we denote by $Q(R)$ its field of fractions.

2. DEFINITION OF VALUATIONS

Let K be a field.

Definition 2.1. A *valuation ring* on K is a subring $\mathcal{O} \subseteq K$ such that for all $x \in K^*$ we have $x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$.

Lemma 2.2. *There is a bijection between the set of valuation rings of K and the set of relations \leq on K^* which satisfy for $x, y, z \in K^*$*

- i. $x \leq y$ or $y \leq x$;
- ii. $x \leq y, y \leq z \implies x \leq z$;
- iii. $x \leq y \implies xz \leq yz$;
- iv. if $x + y \neq 0$, then $x \leq x + y$ or $y \leq x + y$.

This bijection maps a valuation ring \mathcal{O} to the relation which for $x, y \in K^$ is defined by: $x \leq y$ iff $y/x \in \mathcal{O}$. The inverse maps \leq to $\{x \in K^* : 1 \leq x\} \sqcup \{0\}$.*

Proof. Let \mathcal{O} be a valuation ring and consider the obtained relation \leq . Then i holds by definition. Property ii, iii hold as \mathcal{O} is a ring. For iv, suppose that $x \leq y$, that is, $y/x \in \mathcal{O}$. Then we have $1 + y/x = (x + y)/x \in \mathcal{O}$. Hence $x \leq x + y$ as required.

Given \leq , we claim that $\mathcal{O} = \{x \in K^* : 1 \leq x\} \sqcup \{0\}$ is a valuation ring. Let $x \in K^*$. We have $1 \leq 1$ (i) and hence $1 \in \mathcal{O}$. Furthermore, $-1 \in \mathcal{O}$. Indeed, by i we have $1 \leq -1$ or $-1 \leq 1$. In the first case we are done, in the second case we can multiply by -1 to obtain $1 \leq -1$ (iii). Take $x, y \in \mathcal{O} \setminus \{0\}$. Then if we multiply $x \geq 1$ by y we obtain $xy \geq y \geq 1$ (iii), and hence we have $xy \in \mathcal{O}$ (ii). If $x + y \neq 0$, we find $x + y \geq x \geq 1$ or $x + y \geq y \geq 1$. From ii we conclude that $x + y \geq 1$. Take $z \in K^*$. Then we have $1 \leq z$ or $z \leq 1$ (i). In the first case, we have $z \in \mathcal{O}$. In the second case, we multiply by z^{-1} and iv gives $1 \leq z^{-1}$. Hence $z^{-1} \in \mathcal{O}$. This shows that \mathcal{O} is a valuation ring. \square

Let \mathcal{O} be a valuation on K . Consider the relation \leq on K^* induced from \mathcal{O} as in the lemma above. One easily sees that $\mathcal{O}^* = \{x \in K^* : 1 \leq x \text{ and } x \leq 1\}$. Furthermore, if $x, y \in \mathcal{O} \setminus \mathcal{O}^*$, we deduce from property iv and ii that $x + y$ is not a unit. Hence \mathcal{O} is a local ring. The induced relation \leq on K^* makes K^*/\mathcal{O}^* into an *ordered abelian group*. An ordered abelian group is an abelian group P , written additively, together with a relation \leq such that for $a, b, c \in P$ we have:

- i. $a \leq b, b \leq a \implies a = b$;
- ii. $a \leq b, b \leq c \implies a \leq c$;
- iii. $a \leq b$ or $b \leq a$;
- iv. $a \leq b \implies a + c \leq b + c$.

The group morphism $v: K^* \rightarrow K^*/\mathcal{O}^*$ is called the *valuation map* and it satisfies for $x, y \in K^*$ with $x + y \neq 0$: $v(x + y) \geq \min(v(x), v(y))$. The ordered abelian group K^*/\mathcal{O}^* is called the *value group*.

To shorten notation we just write v for a valuation. We denote by \mathcal{O}_v the valuation ring with maximal ideal \mathfrak{m}_v . The residue field is denoted by $k_v = \mathcal{O}_v/\mathfrak{m}_v$. The value group is denoted by $\Delta_v = K^*/\mathcal{O}^*$, for which we use additive notation. We use the notation $v: K^* \rightarrow \Delta_v$. We set

$$p_v = \begin{cases} \text{char}(k_v) & \text{if } \text{char}(k_v) \neq 0 \\ 1 & \text{if } \text{char}(k_v) = 0. \end{cases}$$

A pair (K, v) as above is called a *valued field*. Note that a valuation v gives rise to the valued field $(Q(\mathcal{O}_v), v)$ where $Q(\mathcal{O}_v)$ is the fraction field of \mathcal{O}_v . If K' is a subfield, then we denote by $v|_{K'}$ the valuation on K' corresponding to the valuation ring $\mathcal{O}_v \cap K'$.

3. MAIN RESULTS

In this section we will provide statements of the main results. Proofs of the statements follow in Sections 4, 5, 6 and 7 and will occupy most of this article.

3.1. Properties of extensions of valuations. Let $M \supseteq N$ be an extension of field. When we say that M/N is separable we mean that it is algebraic and separable. Similarly, normal means normal and algebraic (but not necessarily separable). Assume that M/N is finite. We set $[M : N]_s$ for the separability degree of the extension and $[M : N]_i$ for the inseparability degree. Note that $[M : N] = [M : N]_s \cdot [M : N]_i$.

Let (K, v) be a valued field and let L be an extension of K . An *extension* of v to L is a valuation w on L satisfying $\mathcal{O}_w \cap K = \mathcal{O}_v$, equivalently, $\mathfrak{m}_w \cap K = \mathfrak{m}_v$. Such extensions do exist (Proposition 5.6). We denote such an extension by $(L, w) \supseteq (K, v)$ or $w|v$. Sometimes we write $w|v$ if w extends v . The number of extensions of v to L is denoted by $g_{L,v}$, which is finite if L/K is finite (Proposition 5.6). Such an extension $(L, w) \supseteq (K, v)$ is called *finite* if L/K is finite. In a similar way we define such an extension to be normal, separable, An extension induces inclusions $\Delta_v \rightarrow \Delta_w$ and $\mathfrak{k}_v \rightarrow \mathfrak{k}_w$. The following proposition defines a lot of quantities relating to a finite extension of valued fields and gives some properties of these quantities (see Proposition 7.1).

Proposition 3.1. *Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Then one has:*

- $e(w/v) := (\Delta_w : \Delta_v) \in \mathbf{Z}_{\geq 1}$ (ramification index);
- $e_t(w/v) := \text{lcm}\{m \in \mathbf{Z}_{\geq 1} : m|e(w/v), \gcd(m, p_v) = 1\} \in \mathbf{Z}_{\geq 1}$ (tame ramification index);
- $e_w(w/v) := \frac{e(w/v)}{e_t(w/v)} \in p_v^{\mathbf{Z}_{\geq 0}}$ (wild ramification index);
- $f(w/v) := [\mathfrak{k}_w : \mathfrak{k}_v] \in \mathbf{Z}_{\geq 1}$ (residue field degree);
- $f_s(w/v) := [\mathfrak{k}_w : \mathfrak{k}_v]_s \in \mathbf{Z}_{\geq 1}$ (separable residue field degree);
- $f_i(w/v) := [\mathfrak{k}_w : \mathfrak{k}_v]_i \in p_v^{\mathbf{Z}_{\geq 0}}$ (inseparable residue field degree);
- Let M/K be a finite normal extension containing L . We define the local degree by $n(w/v) := \frac{g_{M,w}}{g_{M,v}} \cdot [L : K] \in \mathbf{Z}_{\geq 1}$ and this does not depend on the choice of M ;
- $d(w/v) := \frac{n(w/v)}{e(w/v)f(w/v)} \in p_v^{\mathbf{Z}_{\geq 0}}$ (defect);
- $d_w(w/v) := d(w/v)e_w(w/v)f_i(w/v) \in p_v^{\mathbf{Z}_{\geq 0}}$ (wildness index);

The quantities e , e_t , e_w , f , f_s , f_i , n , d and d_w are multiplicative in towers.

Definition 3.2. Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Then we have the following properties which $(L, w) \supseteq (K, v)$ can satisfy:

- *immediate*: $d_w(w/v) = e_t(w/v) = f_s(w/v) = 1$, equivalently, $n(w/v) = 1$;
- *unramified*: $d_w(w/v) = e_t(w/v) = 1$;
- *tame*: $d_w(w/v) = 1$;
- *local*: $g_{L,v} = 1$;
- *totally ramified*: $f_s(w/v) = g_{L,v} = 1$;
- *totally wild*: $e_t(w/v) = f_s(w/v) = g_{L,v} = 1$.

We say that v is *totally split* in L if $g_{L,v} = [L : K]$.

As the various degrees are multiplicative, we can extend this definition in the following way. Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields. Then $w|v$ is *immediate* (respectively *unramified*, *tame*, *local*, *totally ramified*, *totally wild*) if all intermediate extensions (L', w') of $(L, w) \supseteq (K, v)$ where L'/K is finite are immediate (respectively unramified, tame, local, totally ramified, totally wild). We say that v is *totally split* in L if all intermediate extensions (L', w') of $(L, w) \supseteq (K, v)$ with L'/K finite are totally split.

3.2. Normal extensions.

Definition 3.3. Let $(M, x) \supseteq (K, v)$ be a normal algebraic extension of valued fields and let $G = \text{Aut}_K(M)$. Note that G acts on the set of valuations on M extending v by $\mathcal{O}_{g(x')} = g(\mathcal{O}_{x'})$. Let $D_{x,K} = \{g \in G : gx = x\}$ be the *decomposition*

group of x over K . We define the *inertia group* $I_{x,K} \subseteq D_{x,K}$ of x over K to be the kernel of the natural group morphism $D_{x,K} \rightarrow \text{Aut}_{k_v}(k_x)$. Furthermore, there is a natural group morphism

$$I_{x,K} \rightarrow \text{Hom}(\Delta_x/\Delta_v, k_x^*)$$

$$\bar{c} \mapsto \frac{\overline{g(c)}}{c}$$

(see Lemma 6.3). We define the *ramification group* of x over K to be its kernel. We denote it by $V_{x,K}$.

Let $\Gamma_{x,v} = \text{im}(\text{Aut}_{k_v}(k_x) \rightarrow \text{Aut}_{k_v^*}(k_x^*))$. Let $\text{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ be the subgroup of $\text{Aut}(M^*/(1+\mathfrak{m}_x))$ consisting of those automorphisms such that the restriction to k_x^* lies in $\Gamma_{x,v}$ and which are the identity on $K^*/(1+\mathfrak{m}_v)$. We have a natural map $D_{x,K} \rightarrow \text{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ (see the discussion after Lemma 6.3).

We endow G with the profinite topology. This means that we view G as a subset of M^M . We endow M with the discrete topology, M^M with the product topology and G with the induced topology. Similarly we define profinite topologies on $\text{Aut}_{k_v}(k_x) \subseteq k_x^{k_x}$ and $\text{Hom}(\Delta_x/\Delta_v, k_x^*) \subseteq (k_x^*)^{\Delta_x/\Delta_v}$ where k_x and k_x^* have the discrete topology. Furthermore, let S be the set of valuations extending v to M . For $x' \in S$ and a finite extension L of K in M we set $U_{x',L} = \{x'' \in S : x''|_L = x'|_L\}$. This is a basis for a topology on S . We give $\text{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ the following topology. We give $C = M^*/(1+\mathfrak{m}_x)$ the discrete topology, C^C the product topology and $\text{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$ the induced topology.

Definition 3.4. Let L/K be a field extension. We set $L_{K,\text{sep}}$ for the field extension of K consisting of the elements in L which are separable and algebraic over K .

Definition 3.5. Let $(M, x) \supseteq (K, v)$ be a normal algebraic extension of valued fields. We define $K_{h,x} = M_{K,\text{sep}}^{D_{x,K}}$ (*decomposition field*, h stands for Henselization), $K_{i,x} = M_{K,\text{sep}}^{I_{x,K}}$ (*inertia field*) and $K_{v,x} = M_{K,\text{sep}}^{V_{x,K}}$ (*ramification field*). Note that all these extensions are separable over K and that we have $K \subseteq K_{h,x} \subseteq K_{i,x} \subseteq K_{v,x} \subseteq M$.

Recall that for a prime p and a profinite group H a pro- p -Sylow subgroup H' is a maximal subgroup of H such that H' is a projective limit of finite groups of p -power order.

We define the *Steinitz monoid* as the following set. Let $\mathcal{P} \subset \mathbf{Z}$ be the set of primes. *Steinitz numbers* are of the form $\prod_{p \in \mathcal{P}} p^{n_p}$ with $n_p \in \mathbf{Z}_{\geq 0} \sqcup \{\infty\}$. This set has an obvious monoid structure and there is an obvious way for defining gcd and lcm for arbitrary sets of Steinitz numbers. Furthermore, there is an obvious notion of divisibility.

Let H be a profinite group. Then we define its *order* to be

$$\text{ord}(H) = \text{lcm}\{[H : N] : N \text{ open normal subgroup of } H\},$$

and we define its *exponent* to be

$$\exp(H) = \text{lcm}\{\exp(H/N) : N \text{ open normal subgroup of } H\}.$$

Both are Steinitz numbers. Furthermore, if $H = \varprojlim_{i \in I} H_i$ where the H_i are finite, then one has $\text{ord}(H) = \text{lcm}(\text{ord}(H_i) : i \in I)$ and $\exp(H) = \text{lcm}(\exp(H_i) : i \in I)$.

The proof of the following theorem can be found on Page 21.

Theorem 3.6. *Let $(M, x) \supseteq (K, v)$ be a normal algebraic extension of valued fields and let $G = \text{Aut}_K(M)$. Then G acts continuously on the set S consisting of the valuations of M extending K and induces an isomorphism of topological G -sets*

$$G/D_{x,K} \rightarrow S$$

$$\bar{g} \mapsto gx.$$

For $g \in G$ one has $D_{g(x),K} = gD_{x,K}g^{-1}$, $I_{g(x),K} = gI_{x,K}g^{-1}$ and $V_{g(x),K} = gV_{x,K}g^{-1}$. One also has $K_{h,g(x)} = gK_{h,x}$, $K_{i,g(x)} = gK_{i,x}$ and $K_{v,g(x)} = gK_{v,x}$.

Furthermore, we have exact sequences of profinite groups

$$0 \rightarrow I_{x,K} \rightarrow D_{x,K} \rightarrow \text{Aut}_{k_v}(k_x) \rightarrow 0,$$

$$0 \rightarrow V_{x,K} \rightarrow I_{x,K} \rightarrow \text{Hom}(\Delta_x/\Delta_v, k_x^*) \rightarrow 0$$

and

$$0 \rightarrow V_{x,K} \rightarrow D_{x,K} \rightarrow \text{Aut}_{K^*, \Gamma_{x,v}}(M^*/(1 + \mathfrak{m}_x)) \rightarrow 0.$$

The extension k_x/k_v is normal and $V_{x,K}$ is the unique pro- p_v -Sylow subgroup of $I_{x,K}$. Then for any integer $r \in \mathbf{Z}_{\geq 1}$ dividing $\exp(I_{x,K}/V_{x,K})$ the field k_x contains a primitive r -th root of unity.

Let (L, w) be an intermediate extension of $(M, x) \supseteq (K, v)$ and let $H = \text{Aut}_L(M)$. Then one has:

- i. $D_{x,L} = D_{x,K} \cap H$, $I_{x,L} = I_{x,K} \cap H$ and $V_{x,L} = V_{x,K} \cap H$;
- ii. $L_{h,x} = K_{h,x}L$, $L_{i,x} = K_{i,x}L$ and $L_{v,x} = K_{v,x}L$.

If in addition we assume that L/K is normal, then we have exact sequences

$$0 \rightarrow D_{x,L} \rightarrow D_{x,K} \rightarrow D_{w,K} \rightarrow 0,$$

$$0 \rightarrow I_{x,L} \rightarrow I_{x,K} \rightarrow I_{w,K} \rightarrow 0,$$

and

$$0 \rightarrow V_{x,L} \rightarrow V_{x,K} \rightarrow V_{w,K} \rightarrow 0.$$

Under the normality assumption we have $K_{h,x|L} = K_{h,x} \cap L$, $K_{i,x|L} = K_{i,x} \cap L$ and $K_{v,x|L} = K_{v,x} \cap L$.

If the extension M/K is finite, the previous theorem implies the following (proof on Page 24).

Proposition 3.7. *Let $(M, x) \supseteq (K, v)$ be a finite normal extension of valued fields. Then one has*

$$\begin{aligned} [K_{h,x} : K] &= g_{M,v} \\ [K_{i,x} : K_{h,x}] &= f_s(x/v) = f_s(x|_{K_{i,x}}/x|_{K_{h,x}}) \\ [K_{v,x} : K_{i,x}] &= e_t(x/v) = e_t(x|_{K_{v,x}}/x|_{K_{i,x}}) \\ [M : K_{v,x}] &= d_w(x/v) = d_w(x|_{K_{v,x}}). \end{aligned}$$

Let (L, w) be an intermediate extension of $(M, x) \supseteq (K, v)$. Then one has

$$\begin{aligned} [L_{h,x} : K_{h,x}] &= d_w(w/v) e_t(w/v) f_s(w/v) \\ [L_{i,x} : K_{i,x}] &= d_w(w/v) e_t(w/v) \\ [L_{v,x} : K_{v,x}] &= d_w(w/v). \end{aligned}$$

The proof of the following theorem can be found on Page 23.

Theorem 3.8. *Let $(M, x) \supseteq (K, v)$ be a normal extension of valued fields. Then the following hold.*

- i. *Assume that k_x has no cyclic extensions of prime order dividing the order of $I_{x,K} / V_{x,K}$. Then the exact sequence*

$$0 \rightarrow I_{x,K} / V_{x,K} \rightarrow D_{x,K} / V_{x,K} \rightarrow D_{x,K} / I_{x,K} \rightarrow 0$$

is right split.

- ii. *Assume that k_x has no cyclic extensions of prime order dividing p_v or that $p_v \nmid \text{ord}(I_{x,K})$. Then the exact sequence*

$$0 \rightarrow V_{x,K} \rightarrow D_{x,K} \rightarrow D_{x,K} / V_{x,K} \rightarrow 0$$

is right split.

- iii. *Assume that k_x has no cyclic extensions of prime order dividing $\text{ord}(I_{x,K})$. Then the exact sequence*

$$0 \rightarrow I_{x,K} \rightarrow D_{x,K} \rightarrow D_{x,K} / I_{x,K} \rightarrow 0$$

is right split.

3.3. Algebraic extensions. A well-known result in the following (proof on Page 24).

Theorem 3.9 (Fundamental equality). *Let (K, v) be a valued field and let L/K be a finite field extension. Then we have*

$$\begin{aligned} [L : K] &= \sum_{w|v \text{ on } L} n(w/v) = \sum_{w|v \text{ on } L} d(w/v) e(w/v) f(w/v) \\ &\geq \sum_{w|v \text{ on } L} e(w/v) f(w/v). \end{aligned}$$

Two algebraic field extensions L, L' of a field K are called *linearly disjoint* over K if $L \otimes_K L'$ is a field.

If L, L' are subfields of a field Ω , then we set the *compositum* $LL' = \text{im}(L \otimes_{\mathbf{Z}} L' \rightarrow \Omega)$. This is the smallest ring containing both L and L' in Ω . This is a field if the elements of L are algebraic over L' or if the elements of L' are algebraic over L .

The following proposition studies extensions of valuations using fundamental sets (Proof on 25). If $L \supseteq K$ and $M \supseteq K$ are extensions of fields, we denote by $\text{Hom}_K(L, M)$ the set of field homomorphisms from L to M which are the identity on K .

Theorem 3.10. *Let (K, v) be a valued field and let L/K be an algebraic extension. Let $(M, x) \supseteq (K, v)$ be a normal extension with group $G = \text{Aut}_K(M)$ such that the G -set $X = \text{Hom}_K(L, M)$ is not empty. Then the natural map*

$$\begin{aligned} \pi : X &\rightarrow \{w \text{ on } L \text{ extending } v\} \\ \sigma &\mapsto w \text{ s.t. } \mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L)) \end{aligned}$$

is surjective. Let $\sigma \in X$ and set $w = \pi(\sigma)$ and let G_σ be the stabilizer in G of σ . Then we have:

- i. w/v is immediate $\iff \sigma(L) \subseteq K_{h,x} \iff D_{x,K} \subseteq G_\sigma$;
- ii. w/v is unramified $\iff \sigma(L) \subseteq K_{i,x} \iff I_{x,K} \subseteq G_\sigma$;
- iii. w/v is tame $\iff \sigma(L) \subseteq K_{v,x} \iff V_{x,K} \subseteq G_\sigma$;

- iv. w/v is local $\iff \sigma(L)$ and $K_{h,x}$ are linearly disjoint over $K \iff D_{x,K} \sigma = X$;
- v. w/v is totally ramified $\iff \sigma(L)$ and $K_{i,x}$ are linearly disjoint over $K \iff I_{x,K} \sigma = X$;
- vi. w/v is totally wild $\iff \sigma(L)$ and $K_{v,x}$ are linearly disjoint over $K \iff V_{x,K} \sigma = X$.

Furthermore we have:

- vii. x/w is immediate $\iff M = \sigma(L)K_{h,x} \iff M/\sigma(L)$ is separable and $G_\sigma \cap D_{x,K} = 0$;
- viii. x/w is unramified $\iff M = \sigma(L)K_{i,x} \iff M/\sigma(L)$ is separable and $G_\sigma \cap I_{x,K} = 0$;
- ix. x/w is tame $\iff M = \sigma(L)K_{v,x} \iff M/\sigma(L)$ is separable and $G_\sigma \cap V_{x,K} = 0$;
- x. x/w is local $\iff \sigma(L) \supseteq K_{h,x} \iff G_\sigma \subseteq D_{x,K}$;
- xi. x/w is totally ramified $\iff \sigma(L) \supseteq K_{i,x} \iff G_\sigma \subseteq I_{x,K}$;
- xii. x/w is totally wild $\iff \sigma(L) \supseteq K_{v,x} \iff G_\sigma \subseteq V_{x,K}$.

Finally we have:

- xiii. v is totally split in $L \iff$ for all $\sigma \in X$ we have $\sigma(L) \subseteq K_{h,x} \iff D_{x,K}$ acts trivially on X ;
- xiv. w is totally split in $M \iff M/\sigma(L)$ is separable and only the trivial element of G_σ is conjugate to an element of $D_{x,K}$.

The above proposition has a lot of corollaries. The proof of the first corollary can be found on Page 25.

Corollary 3.11. *Let (K, v) be a valued field and let L and L' be two algebraic extensions of K in some algebraic closure of K . Let x be a valuation on LL' extending v and let $w = x|_L$ and $w' = x|_{L'}$. Then the following statements hold:*

- i. *if w/v is immediate, then x/w' is immediate;*
- ii. *if w/v is unramified, then x/w' is unramified;*
- iii. *if w/v is tame, then x/w' is tame;*
- iv. *if v is totally split in L , then w' is totally split in LL' .*

The proof of the following corollary can be found on Page 26.

Corollary 3.12. *Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields and let (K', w') be an intermediate extension. Then w/v is immediate (respectively unramified, tame, local, totally ramified, totally wild) iff w/w' and w'/v are immediate (respectively unramified, tame, local, totally ramified, totally wild).*

The proof of the following proposition can be found on Page 11.

Proposition 3.13. *Let Ω be a field and let $L, L' \subseteq \Omega$ be subfields. Then there is a subfield M of L such that for all subfields F of L the natural map $L \otimes_F (L'F) \rightarrow LL'$ is an isomorphism iff $M \subseteq F$. Furthermore, M can be described in the following two ways, where \mathbf{F} is the prime field of Ω .*

- i. *Let $\mathfrak{B} \subseteq L'$ be a basis of LL' over L . For $b \in \mathfrak{B}$ and $x \in L'$ write $x = \sum_{b \in \mathfrak{B}} c_{x,b}b$ with $c_{x,b} \in L$ almost all zero. Then one has $M = \mathbf{F}(c_{x,b} : x \in L', b \in \mathfrak{B})$.*

ii. Set

$$S = \{c \in L : \exists I \subseteq L' \text{ finite, ind. over } L \text{ and } (c_i)_{i \in I} \in L^I \\ \text{s.t. } \exists i \in I \text{ s.t. } c_i = c \text{ and } \sum_{i \in I} c_i i \in L'\}.$$

Then one has $M = \mathbf{F}(S)$.

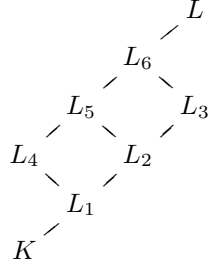
Definition 3.14. The field M in the above theorem is called the *field of definition* of L' over L and is denoted by $L \searrow L'$.

The proof of the following theorem can be found on Page 26.

Theorem 3.15. Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields. Then the following statements hold:

- i. There is a unique maximal subextension L_1 of L/K such that $w|_{L_1}/v$ is immediate (respectively L_2 for unramified and L_3 for tame).
- ii. There is a unique minimal subextension L_4 of L/K such that $w/w|_{L_4}$ is local (respectively L_5 for totally ramified and L_6 for totally wild).

We have the following diagram of inclusions:



For any $(M, x) \supseteq (L, w) \supseteq (K, v)$ extension of valued fields where M/K is normal, we have $L_1 = K_{h,x} \cap L$, $L_2 = K_{i,x} \cap L$ and $L_3 = K_{v,x} \cap L$, $L_4 = L_{K,\text{sep}} \searrow K_{h,x}$, $L_5 = L_{K,\text{sep}} \searrow K_{i,x}$ and $L_6 = L_{K,\text{sep}} \searrow K_{v,x}$.

If there is a normal extension M/K containing L such that $g_{M,w} = 1$, then $L_1 = L_4$, $L_2 = L_5$ and $L_3 = L_6$.

The proof of the following corollary can be found on Page 27.

Corollary 3.16. Let (K, v) be a valued field and let L and L' be two algebraic extensions contained in an algebraic extension L'' of K . Let x be a valuation on L'' extending v and let $w = x|_L$ and $w' = x|_{L'}$. Assume that $K = L \cap L'$ and there exists a normal extension M/K containing LL' such that $g_{M,w} = 1$. Then the following statements hold:

- i. if x/w' is local, then w/v is local;
- ii. if x/w' is totally ramified, then w/v is totally ramified;
- iii. if x/w' is totally wild, then w/v is totally wild.

The proof of the following proposition can be found on Page 28.

Proposition 3.17. Let (K, v) be a valued field and let L be a finite separable algebraic extension of K . Let $(M, x) \supseteq (K, v)$ be a finite normal extension of

valued fields with group $G = \text{Aut}_K(M)$ such that the G -set $X = \text{Hom}_K(L, M)$ is not empty. Then the map

$$\begin{aligned} \varphi: D_{x,K} \setminus X &\rightarrow \{w \text{ of } L \text{ extending } v\} \\ D_{x,K} s &\mapsto w \text{ s.t. } \mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L)) \end{aligned}$$

is a bijection of sets. If $\varphi(D_{x,K} s) = w$ we have:

- i. $\# D_{x,K} s = d_w(w/v) e_t(w/v) f_s(w/v) = n(w/v)$;
- ii. the number of orbits under $I_{x,K}$ of $D_{x,K} s$ is equal to $f_s(w/v)$ and each orbit has length $d_w(w/v) e_t(w/v)$;
- iii. the number of orbits under $V_{x,K}$ of $D_{x,K} s$ is equal to $e_t(w/v) f_s(w/v)$ and each orbit has length $d_w(w/v)$.

The proof of the following corollary can be found on Page 28

Corollary 3.18. *Let (K, v) be a valued field and let L be a finite algebraic extension of K . Let $(M, x) \supseteq (K, v)$ be a finite normal extension of valued fields with group $G = \text{Aut}_K(M)$ such that the G -set $X = \text{Hom}_K(L, M)$ is not empty. Then the cardinality of the set of valuations w on L extending v such that $f_s(w/v) = 1$ is equal to $\#(I_{x,K} \setminus X)^{D_{x,K} / I_{x,K}}$.*

4. PRELIMINARIES

4.1. Field theory.

4.1.1. *Linearly disjoint extensions.* Let Ω be a field and let $L, L' \subseteq \Omega$. We set $LL' = \text{im}(L \otimes_{\mathbf{Z}} L' \rightarrow \Omega)$, that is, the smallest ring containing both L and L' . This is a field if the elements of L are algebraic over L' or if the elements of L' are algebraic over L .

Two algebraic field extensions L, L' of a field K are called *linearly disjoint* over K if $L \otimes_K L'$ is a field. This holds if and only if all pairs of finite subextensions of L/K respectively L'/K are linearly disjoint over K .

Let M/K is a normal field extension with group $G = \text{Aut}_K(M)$. Then the latter group is a topological group with the topology coming from viewing $G \subset M^M$ where M has the discrete topology and M^M the product topology.

Lemma 4.1. *Let M/K be a normal extension of fields with group $G = \text{Aut}_K(M)$ and let L, L' be two intermediate extensions. Put $H = \text{Aut}_L(M)$ and $H' = \text{Aut}_{L'}(M)$. Then one has: $\overline{\langle H, H' \rangle} = G$ iff $L \cap L'$ over K is purely inseparable.*

Proof. Set $p = \text{char}(K)$ if $\text{char}(K)$ is positive and 1 otherwise. It is very easy to see that $M_{L,\text{ins}} \cap M_{L',\text{ins}} = M_{L \cap L',\text{ins}}$. Note that $H = \text{Aut}_{M_{L,\text{ins}}}(M)$, $H' = \text{Aut}_{M_{L',\text{ins}}}(M)$ and $G = \text{Aut}_{M_{K,\text{ins}}}(M)$ and that M is Galois over $M_{K,\text{ins}}$, $M_{L,\text{ins}}$ and $M_{L',\text{ins}}$ (Proposition 4.9). From Galois theory it follows that $\overline{\langle H, H' \rangle}$ corresponds to $M_{L,\text{ins}} \cap M_{L',\text{ins}} = M_{L \cap L',\text{ins}}$ and that G corresponds to $M_{K,\text{ins}}$. Hence one has: $\overline{\langle H, H' \rangle} = G$ iff $M_{L \cap L',\text{ins}} = M_{K,\text{ins}}$ iff $L \cap L'/K$ is purely inseparable. \square

For a field K we denote by K_{sep} its separable closure.

Proposition 4.2. *Let M/K be a normal extension of fields with group $G = \text{Aut}_K(M)$ and let L, L' be two intermediate extensions. Put $H = \text{Aut}_L(M)$ and $H' = \text{Aut}_{L'}(M)$. Assume that L/K is separable. Then the following statements are equivalent:*

- i. L and L' are linearly disjoint over K ;
- ii. $L \otimes_K L'$ is a domain;
- iii. the natural map $L \otimes_K L' \rightarrow LL'$ is an isomorphism;
- iv. $G = H \cdot H'$;
- v. H' acts transitively on G/H ;
- vi. the natural map $\text{Hom}_{L'}(LL', K_{\text{sep}}) \rightarrow \text{Hom}_K(L, K_{\text{sep}})$ is a bijection.

If L/K or L'/K is normal, then the above statements are equivalent to $L \cap L' = K$.

Proof. i \iff ii: One implication is obvious. Suppose that $L \otimes_K L'$ is a domain. To show that every element has an inverse, we may reduce to the case where both L/K and L'/K are finite. The result follows since a domain which is finite over a field is a field.

i \iff iii: Obvious.

iv \iff v: Obvious.

v \iff vi: The map in vi is the natural injective map $H'/\langle H \cap H' \rangle \rightarrow G/H$. It is surjective iff H' acts transitively on G/H .

i \implies vi: The natural map $\text{Hom}_{L'}(LL', K_{\text{sep}}) \rightarrow \text{Hom}_K(L, K_{\text{sep}})$ is injective. Let $\varphi \in \text{Hom}_K(L, K_s)$ be given. Let L'' be a finite extension of K contained in L . Since L and L' are disjoint over K , we find $[LL' : L'] = [L : K]$. This shows, since L/K is separable, that the natural injective map $\text{Hom}_{L'}(L''L', K_{\text{sep}}) \rightarrow \text{Hom}_K(L'', K_{\text{sep}})$ is a bijection. Hence there is a unique morphism of fields in $\text{Hom}_{L'}(L''L', K_s)$ mapping to $\varphi|_{L''}$. By uniqueness we can glue these morphisms to a unique morphism mapping to φ .

iv \implies i: If $G = H \cdot H'$, then for any finite subextension of L/K the same holds. Hence all finite extensions of L/K are linearly disjoint from L' . But then it easily follows that L and L' are linearly disjoint over K .

We will now prove the last part. If $L \otimes_K L'$ is a field, then obviously we have $L \cap L' = K$. For the other implication, assume first that L/K is normal. This means that $H = \ker(\text{Aut}_K(M) \rightarrow \text{Aut}_K(L))$ is a normal subgroup of G . But then one easily sees that $H \cdot H' = \langle H, H' \rangle$. A similar statement holds if L'/K is normal. Furthermore, as H and H' are compact groups, one sees that $H \cdot H'$ is closed. Hence $\overline{\langle H, H' \rangle} = H \cdot H'$. From 4.1, as L/K is separable, it follows that $H \cdot H' = \overline{\langle H, H' \rangle} = G$. The result follows. \square

Proof of Proposition 3.13. Let \mathfrak{L} be the set of subfields F of L such that the natural map $L \otimes_F L'F \rightarrow LL'$ is an isomorphism. Consider the notation from i. Directly from the definitions it follows that for a subfield F of L we have $F \in \mathfrak{L}$ iff \mathfrak{B} spans $L'F$ as F -vector space. But $L'F$ is generated as an F -vector space by L' and each $x \in L'$ can be written in a unique way as $x = \sum_{b \in \mathfrak{B}} c_{x,b}b$ where $c_{x,b} \in L$ and almost all $c_{x,b}$ are 0. Let \mathbf{F} be the primefield of L . Hence we conclude that $F \in \mathfrak{L}$ iff for all $x \in L$ and $b \in \mathfrak{B}$ we have $c_{x,b} \in F$ iff F contains $M = \mathbf{F}(c_{x,b} : x \in L, b \in \mathfrak{B})$. Description ii follows directly from description one since we can extend an independent set to a basis. \square

Definition 4.3. The field M in the above theorem is called the *field of definition* of L' over L and is denoted by $L \searrow L'$.

We deduce some properties of $L \searrow L'$.

Lemma 4.4. Let Ω be a field and let $L, L' \subseteq \Omega$ be subfields. Then the following hold:

- i. $L \cap L' \subseteq L \setminus L'$;
- ii. $L \cap L' = L \setminus L'$ iff $L \cap L' = L' \setminus L$ iff $L \setminus L' = L' \setminus L$.

Proof. i: Suppose $x \in L \cap L' \setminus L \setminus L'$. Then the nonzero element $x \otimes 1 - 1 \otimes x$ maps to zero under $L \otimes_{L \setminus L'} (L \setminus L')L' \rightarrow LL'$, contradiction.

ii: By symmetry, it suffices to show that the first and last statement are equivalent. Suppose that $L \cap L' = L \setminus L'$. Then one has an isomorphism $L \otimes_{L \cap L'} (L \cap L')L' \rightarrow LL'$ and from i one deduces that $L' \setminus L = L' \cap L = L \setminus L'$. Suppose $L \setminus L' = L' \setminus L$. Then one has $L \setminus L' \subseteq L \cap L'$ and the result follows from i. \square

Lemma 4.5. *Let G be a group and let $H, H' \subseteq G$ be subgroups. Let J' be a subgroup of HH' containing H . Then H acts transitively on $J'/J' \cap H'$ if and only if J' is contained in the group $\{g \in G : gHH' = HH'\}$.*

Proof. First notice $J'/J' \cap H' \cong J'(H'/H') \subseteq G/H'$ (as J' -sets). Put $x = H'/H'$. Hence we need to find the largest J' such that H acts transitively on $J'x$, that is $Hx = J'x$. Notice that $J = \{g \in G : gHH' = HH'\} = \{g \in G : gHx = Hx\}$. If H acts transitively on $J'x$, we have for $j' \in J'$:

$$j'Hx = j'J'x = J'x = Hx,$$

hence $j' \in J$. Conversely, J is a subgroup containing H with the property that $Jx = JHx = Hx$. \square

Proposition 4.6. *Let L, L' be subfields of a field Ω . Assume that $L/L \cap L'$ is separable. Let M be a normal extension of $L \cap L'$ containing LL' with groups $G = \text{Aut}_{L \cap L'}(M)$, $H = \text{Aut}_L(M)$ and $H' = \text{Aut}_{L'}(M)$. Let $J = \{g \in G : gHH' = HH'\}$. Then one has:*

$$L \setminus L' = (LL')^J \cap L.$$

Proof. Proposition 4.2 shows that we need to find a maximal subgroup $J' \subseteq HH'$ containing H such that H acts transitively on $J'/J' \cap H'$. The unique maximal subgroup with this property is J (Lemma 4.5). It remains to show that J is a closed subgroup. Notice that H and H' are compact, and hence that HH' is compact (because it is the image of $H \times H'$ under the map $G \times G \rightarrow G$) and since we are in a Hausdorff space, it is closed. Similarly, $H'H$ is compact and hence closed. Note that the translation maps are continuous. One then has

$$J = \bigcap_{\tau \in HH'} (\tau H' H \cap HH' \tau^{-1}).$$

Hence J is an intersection of closed subgroups, and hence closed. \square

4.1.2. *Separably disjoint extensions.* Let L/K be an algebraic extension of fields and let p be the characteristic of K if this is nonzero, and 1 otherwise. Then we put

$$L_{K,\text{ins}} = \{x \in L : \exists j \in \mathbf{Z}_{\geq 0} : x^{p^j} \in K\},$$

the maximal purely inseparable field extension of K in L . Notice that $L_{K,\text{ins}} \cap L_{K,\text{sep}} = K$.

Definition 4.7. An algebraic field extension L/K is called *separably disjoint* if $L = L_{K,\text{sep}}L_{K,\text{ins}}$.

Lemma 4.8. *Let L/K be an algebraic extension of valued fields. Then L/K is separably disjoint if and only if $L/L_{K,\text{ins}}$ is separable.*

Proof. \Rightarrow : Follows directly from the definitions.

\Leftarrow : Note that $L/L_{K,\text{sep}}$ is purely inseparable and hence $L/L_{K,\text{sep}}L_{K,\text{ins}}$ is purely inseparable and separable. It follows that $L = L_{K,\text{sep}}L_{K,\text{ins}}$. \square

Proposition 4.9. *Let L/K be a normal extension of fields. Then L/K is separably disjoint.*

Proof. See [Lan02, Chapter V, Proposition 6.11].

Here is a similar proof. Take $x \in L \setminus L_{K,\text{ins}}$. As x is not purely inseparable over $L_{K,\text{ins}}$ and as L/K is normal, there is an element of $\text{Aut}_K(L)$ which does not fix x (use Zorn to find such a morphism). Hence $L^{\text{Aut}_K(L)} = L_{K,\text{ins}}$ and from Galois theory it follows that $L/L_{K,\text{ins}}$ is separable. Apply Lemma 4.8. \square

Notice that any algebraic field extension L/K has a unique maximal separably disjoint subextension, namely $L_{K,\text{sep}}L_{K,\text{ins}}$.

Proposition 4.10. *Let L/K be an algebraic extension of fields. Then*

$$\begin{aligned} \varphi: \{E : K \subseteq E \subseteq L\} &\rightarrow \{(D, F) : K \subseteq D \subseteq L_{K,\text{sep}} \subseteq F \subseteq L, F/D \text{ sep. disjoint}\} \\ E &\mapsto (E_{K,\text{sep}}, EL_{K,\text{sep}}) \end{aligned}$$

is a bijection with inverse

$$(D, F) \mapsto F_{D,\text{ins}}.$$

Proof. First we show that φ is well-defined. Notice that $E/E_{K,\text{sep}}$ is purely inseparable and that $L_{K,\text{sep}}/E_{K,\text{sep}}$ is separable. Hence we find that $EL_{K,\text{sep}}/E_{K,\text{sep}}$ is separably disjoint.

Let ψ be the proposed inverse as above. We have $\psi(\varphi(E)) = (EL_{K,\text{sep}})_{E_{K,\text{sep}},\text{ins}}$, and this is equal to E since it obviously contains E and $EL_{K,\text{sep}}/E$ is separable. Conversely we have $\varphi(\psi((D, F))) = ((F_{D,\text{ins}})_{K,\text{sep}}, F_{D,\text{ins}}L_{K,\text{sep}})$. One directly finds $(F_{D,\text{ins}})_{K,\text{sep}} = D$. As F/D is separably disjoint, we find $F_{D,\text{ins}}L_{K,\text{sep}} = F$. This shows that both maps are inverse to each other. \square

4.2. Tate's lemma. Let G be a compact topological group which acts continuously on a commutative ring A which is endowed with the discrete topology. This means that the map $G \times A \rightarrow A$ is continuous. For $a \in A$ the map $G \times \{a\} \rightarrow A$ is continuous and the image is compact and hence finite. This shows that all orbits are finite.

Proposition 4.11 (Tate). *Let (G, A) be as above. Let R be a domain and let $\sigma, \tau: A \rightarrow R$ be ring morphisms. Suppose that $\sigma|_{A^G} = \tau|_{A^G}$. Then there exists $g \in G$ such that $\tau = \sigma \circ g$.*

Proof. Let $E \subseteq A$ be a finite set. Let $f_E \in A[Y]$ be a polynomial such that all elements of E occur as coefficients of f_E . Extend the action of G to $A[Y][X]$ by letting G act on the coefficients. We extend $\sigma, \tau: A[Y][X] \rightarrow R[Y][X]$ by $X \mapsto X$, $Y \mapsto Y$. Then consider the polynomial $h_E = \prod_{h' \in Gf_E} (X - h') \in A^G[Y][X]$. We have

$$\prod_{h' \in Gf_E} (X - \sigma(h')) = \sigma(h_E) = \tau(h_E) = \prod_{h' \in Gf_E} (X - \tau(h')).$$

As $R[Y]$ is a domain, we can compare the roots and conclude that there is $g \in G$ such that $\tau(h_E) = \sigma(g(h_E)) \in R[Y][X]$. Hence for this g we have $\tau|_E = \sigma \circ g|_E$.

For any $E \subseteq A$ put $G_E = \{g \in G : \tau|_E = \sigma \circ g|_E\}$. Notice that $G_{\bigcup_i E_i} = \bigcap_i G_{E_i}$ for any collection of subsets $E_i \subseteq A$. For finite E we have shown $G_E \neq \emptyset$. We claim that for finite E the set G_E is closed in G . One easily shows that for $e \in E$ the map $\psi_e : G \rightarrow R$ given by $\psi_e(g) = \sigma(e) - \tau(g(e))$ is continuous. Hence $\psi_e^{-1}(0) = G_{\{e\}}$ is closed. As $G_E = \bigcap_{e \in E} G_{\{e\}}$, the set G_E is closed.

By compactness of G we have $G_A = \bigcap_{E \subseteq A, E \text{ finite}} G_E \neq \emptyset$. This means that there is $g \in G$ such that $\tau = \sigma \circ g$. \square

Corollary 4.12. *Suppose that (G, A) is as above. Let $\mathfrak{p} \subset A^G$ be prime. Then G acts transitively on the set of primes of A lying above \mathfrak{p} .*

Proof. Let $\mathfrak{q}, \mathfrak{q}' \subset A$ be primes lying above \mathfrak{p} . We will now construct two maps from A to $\overline{Q(A^G/\mathfrak{p})}$, the algebraic closure of $Q(A^G/\mathfrak{p})$. Since the orbits of the actions are finite, the extension $Q(A/\mathfrak{q}) \supseteq \overline{Q(A^G/\mathfrak{p})}$ is algebraic. Hence there is a morphism $\sigma : A \rightarrow A/\mathfrak{q} \rightarrow Q(A/\mathfrak{q}) \rightarrow \overline{Q(A^G/\mathfrak{p})}$ which is the identity on A^G/\mathfrak{p} . Similarly one defines another map $\tau : A \rightarrow A/\mathfrak{q}' \rightarrow Q(A/\mathfrak{q}') \rightarrow \overline{Q(A^G/\mathfrak{p})}$. Both maps agree on A^G . Proposition 4.11 says that there is $g \in G$ such that $\tau = \sigma g$. Taking kernels gives $\mathfrak{q}' = \ker \tau = \ker(\sigma g) = g^{-1}(\ker \sigma) = g^{-1}\mathfrak{q}$. We get $g\mathfrak{q}' = \mathfrak{q}$ and this finishes the proof. \square

Corollary 4.13. *Let (G, A) be as above. Let $\mathfrak{q} \subset A$ be a prime lying above a prime $\mathfrak{p} \subset A^G$. Let $G_{\mathfrak{q}/\mathfrak{p}} = \{g \in G : g(\mathfrak{q}) = \mathfrak{q}\}$. Let $l = Q(A/\mathfrak{q})$ and let $k = Q(A^G/\mathfrak{p})$. Then the natural map $G_{\mathfrak{q}/\mathfrak{p}} \rightarrow \text{Aut}_k(l)$ is surjective and l/k is normal algebraic.*

Proof. It is easy to see that l/k is algebraic. Let \overline{k} be an algebraic closure of k containing l . We have a natural map $G_{\mathfrak{q}/\mathfrak{p}} \rightarrow \text{Aut}_k(l) \subseteq \text{Hom}_k(l, \overline{k})$. Let $\varphi \in \text{Hom}_k(l, \overline{k})$. Consider the natural map $\sigma : A \rightarrow Q(A/\mathfrak{q}) = l \subseteq \overline{k}$, which restricts to the natural map $A^G \rightarrow Q(A^G/\mathfrak{p}) = k$. Let $\tau = \varphi\sigma$. Apply Proposition 4.11 to see that there is $g \in G$ with $\varphi\sigma = \sigma g$. But then for $a \in A$ we have

$$g \circ (\sigma(a)) = \sigma(g(a)) = \varphi\sigma(a).$$

This means that g maps σ to σ . It follows that $\text{Aut}_k(l) = \text{Hom}_k(l, \overline{k})$ and hence l/k is normal. \square

4.3. Ordered abelian groups.

Lemma 4.14. *Let (P, \leq) be an ordered abelian group. Let $n \in \mathbf{Z}_{\geq 1}$ and $x, y \in P$. If $nx = ny$, then one has $x = y$. The group P has no non-trivial torsion and $P \otimes_{\mathbf{Z}} \mathbf{Q}$ is an ordered abelian group where we put $x \leq y$ if for all $n \in \mathbf{Z}_{\geq 1}$ such that $nx, ny \in P$ we have $nx \leq ny$.*

Proof. Suppose that $x < y$. Then $x + x < x + y < y + y$, and in a similar fashion, $nx < ny$, which is a contradiction.

If x is torsion, apply the first part to x and 0 to obtain the second result.

The last part is an easy calculation which is left to the reader. \square

Let (P, \leq) and (Q, \leq) be ordered abelian groups. A morphism $\varphi : P \rightarrow Q$ is a group homomorphism respecting the ordering. One easily sees that respecting the order is equivalent to $p \geq 0 \implies \varphi(p) \geq 0$. Indeed, let $p, p' \in P$ with $p \geq p'$. Then we have $p - p' \geq 0$, which gives $\varphi(p) - \varphi(p') = \varphi(p - p') \geq 0$. This gives $\varphi(p) \geq \varphi(p')$.

Lemma 4.15. *Let (P, \leq) be an ordered abelian group and let $\varphi \in \text{Aut}(P)$ such that all orbits are finite. Then φ is the identity.*

Proof. Let $p \in P$ and assume that $\varphi^n(p) = p$. Then one has $p = \varphi^n(p) \geq \dots \geq \varphi(p) \geq p$. Hence we obtain $\varphi(p) = p$. \square

5. EXTENDING VALUATIONS

Lemma 5.1. *Let (K, v) be a valued field. Then \mathcal{O}_v is integrally closed.*

Proof. Suppose $x \in \mathcal{O}_v$ nonzero is integral over \mathcal{O}_v . Then there is a relation $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ with $a_i \in \mathcal{O}_v$ and this shows that $x \in \mathcal{O}_v[x] \cap \mathcal{O}_v[x^{-1}]$. By the definition of a valuation ring we have $\mathcal{O}_v[x] \cap \mathcal{O}_v[x^{-1}] = \mathcal{O}_v$ and the result follows. \square

Proposition 5.2. *Let K be a field. Let $R \subseteq K$ be a subring and let $\mathfrak{p} \in \text{Spec}(R)$. Let $S = \{(A, I) : R \subseteq A \subseteq K, A \text{ ring}, I \subseteq A \text{ ideal}, I \cap R = \mathfrak{p}\}$, ordered by $(A, I) \leq (B, J)$ if $A \subseteq B$ and $I \subseteq J$. Then a pair $(\mathcal{O}, \mathfrak{m})$ is maximal if and only if \mathcal{O} is a valuation ring of K and \mathfrak{m} is its maximal ideal.*

Proof. Let $(\mathcal{O}, \mathfrak{m})$ be a maximal element of S . Notice that $\mathfrak{m}_{\mathfrak{p}} \subset \mathcal{O}_{\mathfrak{p}}$ satisfies $\mathfrak{m}_{\mathfrak{p}} \cap R_{\mathfrak{p}} = \mathfrak{p}R_{\mathfrak{p}}$ and $\mathfrak{m}_{\mathfrak{p}} \cap R = \mathfrak{p}$. Hence by maximality we have $\mathcal{O} = \mathcal{O}_{\mathfrak{p}}$ and $\mathfrak{m} = \mathfrak{m}_{\mathfrak{p}}$. A maximal ideal of \mathcal{O} containing \mathfrak{m} still lies above the maximal ideal of $R_{\mathfrak{p}}$. We conclude that \mathfrak{m} is maximal.

We claim that \mathcal{O} is a valuation ring. Suppose that there is $x \in K^*$ with $x, x^{-1} \notin \mathcal{O}$. From the maximality and the fact that \mathfrak{m} lies above $\mathfrak{p}R_{\mathfrak{p}}$ one obtains $\mathfrak{m}\mathcal{O}[x] = \mathcal{O}[x]$ and $\mathfrak{m}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}]$. Take n, m minimal such that $1 = \sum_{i=0}^n a_i x^i$, $1 = \sum_{i=0}^m b_i x^{-i}$ with $a_i, b_i \in \mathfrak{m}$. Without loss of generality, assume $m \leq n$. Multiply the second equation by x^n , and notice that $1 - b_0 \in \mathcal{O}^*$, to obtain $x^n = \frac{1}{1-b_0} \sum_{i=1}^m b_i x^{n-i}$. Use this relation together with the first relation to see that n is not minimal, contradiction.

Conversely, suppose that \mathcal{O} is a valuation ring of K with maximal ideal \mathfrak{m} , containing R and satisfying $\mathfrak{m} \cap R = \mathfrak{p}$. Suppose that $(\mathcal{O}, \mathfrak{m}) \leq (A, \mathfrak{n})$. Let $x \in A$ nonzero. Then $xx^{-1} = 1 \notin \mathfrak{n}$ and hence $x^{-1} \notin \mathfrak{m}$. As \mathcal{O} is a valuation ring, we obtain $x \in \mathcal{O}$. Hence $(\mathcal{O}, \mathfrak{m})$ is maximal. \square

Since we assume the Axiom of Choice, maximal elements as in Proposition 5.2 exist.

Corollary 5.3. *Let $R \subseteq L$ be a subring where L is a field. Then the intersection of all valuation rings of L containing R in L is the integral closure of R in L .*

Proof. As a valuation ring is integrally closed (Lemma 5.1), the right hand side is contained in the left hand side. Suppose $x \in L$ is not integral over R . Consider the ring $R[x^{-1}]$, which does not contain x as x is not integral. Hence x^{-1} is contained in a maximal ideal $\mathfrak{m} \subset R[x^{-1}]$. Proposition 5.2 gives us a valuation v with $x^{-1} \in \mathfrak{m}_v \cap R[x^{-1}] = \mathfrak{m}$. This is equivalent to $x \notin \mathcal{O}_v$. \square

Proposition 5.4. *Let (K, v) be a valued field and let L/K be an algebraic extension of fields. Let R be the integral closure of \mathcal{O}_v in L . Then there is a bijection between the set of maximal ideals of R and the set of valuations extending v to L , given by $\mathfrak{m} \mapsto R_{\mathfrak{m}}$. The inverse maps a valuation \mathcal{O} with maximal ideal \mathfrak{m} to $\mathfrak{m} \cap R$.*

Proof. Let $\mathfrak{p} \in \text{MaxSpec}(R)$. Then by Proposition 5.2 there exists a valuation ring \mathcal{O}_w of L with $\mathcal{O}_w \supseteq R_{\mathfrak{p}}$ and $\mathfrak{m}_w \cap R = \mathfrak{p}$. We will show $R_{\mathfrak{p}} = \mathcal{O}_w$.

Let $a \in \mathcal{O}_w$ nonzero. As L/K is algebraic, there exists a polynomial $f = \sum_{i=0}^n a_i x^i \in \mathcal{O}_v[x]$ with $f(a) = 0$ and a coefficient which is not in the maximal ideal. Let k minimal such that $a_{k+1}, \dots, a_n \in \mathfrak{m}_v$. Put $f_0 = a_0 + \dots + a_{k-1}x^{k-1}$ and $-f_1 = a_k + \dots + a_n x^{n-k}$. Note that $f_1(a) \in \mathcal{O}_w^*$. Then from $0 = f(a) = f_0(a) - a^k f_1(a)$ we obtain for $b = f_0(a)a^{-k+1} \in \mathcal{O}_v[a^{-1}]$, $c = f_1(a) \in \mathcal{O}_v[a] \setminus \{0\}$ that $a = \frac{b}{c}$. We claim: $b, c \in R$. It is enough to show that b and c are contained in any valuation ring extending R (Corollary 5.3). Let \mathcal{O} be such a valuation ring. If $a \in \mathcal{O}$, then one has $c \in \mathcal{O}$ and hence $b = ac \in \mathcal{O}$. If $a \notin \mathcal{O}$, then one has $a^{-1} \in \mathcal{O}$. Hence $b \in \mathcal{O}$ and $c = ba^{-1} \in \mathcal{O}$. This finishes the proof of the claim. Furthermore, by construction we have $c \notin \mathfrak{m}_w$. Hence $c \notin \mathfrak{m}_w \cap R = \mathfrak{p}$. We see that $a = \frac{b}{c} \in R_{\mathfrak{p}}$. This gives $R_{\mathfrak{p}} = \mathcal{O}_w$ and this shows that the proposed map is well-defined.

Suppose w extends v to L . We want to show that $\mathfrak{m}_w \cap R$ is a maximal ideal of R . But $\mathfrak{m}_w \cap \mathcal{O}_v$ is maximal, and $\mathcal{O}_v \rightarrow R$ is integral. Hence by [AM69, Corollary 5.8] $\mathfrak{m}_w \cap R$ is a maximal ideal of R . This shows that the proposed inverse is well-defined.

Note that for $\mathfrak{p} \in \text{MaxSpec}(R)$ we have $\mathfrak{p} = \mathfrak{p}R_{\mathfrak{p}} \cap R$. Furthermore, we have already seen $R_{\mathfrak{m}_w \cap R} = \mathcal{O}_w$. This shows that both maps are inverse to each other. \square

We will now prove a weak approximation theorem.

Corollary 5.5. *Let (K, v) be a field and let L/K be an algebraic field extension. Let w_1, \dots, w_n be different extensions of v to L . Let $(a_i)_{i=1}^n \in \prod_{i=1}^n \mathcal{O}_{w_i}$ and $r_1, \dots, r_n \in \mathbb{Z}_{\geq 1}$ be given. Then there exists $a \in L$ with $a - a_i \in \mathfrak{m}_{w_i}^{r_i}$ for $i = 1, \dots, n$.*

Proof. Let R be the integral closure of \mathcal{O}_v in L . Proposition 5.4 gives us maximal ideals $\mathfrak{m}_i \in \text{MaxSpec}(R)$ with $R_{\mathfrak{m}_i} = \mathcal{O}_{w_i}$. Using the Chinese remainder theorem, one obtains a surjective map $R \rightarrow \prod_{i=1}^n R/\mathfrak{m}_i^{r_i} = \prod_{i=1}^n \mathcal{O}_{w_i}/\mathfrak{m}_{w_i}^{r_i}$ and the result follows. \square

Proposition 5.6. *Let (K, v) be a valued field and let L/K be a field extension. Then one has $1 \leq g_{L,v}$ and $g_{L,v} = 1$ if L/K is purely inseparable. If (L, x) a finite extension of (K, v) , then one has $e(x/v)f(x/v) \leq [L : K]$ and $g_{L,v}$ is finite. If the extension is normal with group $G = \text{Aut}_K(L)$, then G acts transitively on the set of valuations extending v to L , and $e(x/v)$ and $f(x/v)$ do not depend on the choice of x .*

Proof. The fact that $g_{L,v} \geq 1$ follows from Proposition 5.2.

Assume that L/K is purely inseparable. Let x be an extension of v to L . Then one directly sees $\mathfrak{m}_x = \{r \in L : \exists i : r^{p^i} \in \mathfrak{m}_v\}$. A valuation is determined by its maximal ideal.

Assume that L/K is finite. Take a preimage $S \subseteq L$ of a basis of k_x/k_v and take $T \subseteq L^*$ elements which map bijectively to Δ_x/Δ_v . The one easily sees that ST of cardinality $e(x/v)f(x/v)$ is linearly independent over K and $e(x/v)f(x/v) \leq [L : K]$ follows.

Assume that L/K is normal. The transitivity follows from Corollary 4.12 and Proposition 5.4, and the statements about $e(x/v)$ and $f(x/v)$ are obvious. In particular, if L/K is finite normal, the quantity $g_{L,v}$ is finite. It follows from Proposition 5.2 that $g_{L,v}$ is finite when L/K is finite. \square

Lemma 5.7. *Let (K, v) be a valued field and let L be a finite normal extension of K of degree n . Assume that x is the unique extension of v to L . Then for all $a \in L$ one has $x(a) = \frac{1}{n}v(N_{L/K}(a))$. Furthermore, we have $n\Delta_x \subseteq \Delta_v$.*

Proof. Let $G = \text{Aut}(L/K)$. Then it is well-known that for $a \in L$ one has $N_{L/K}(a) = \left(\prod_{g \in G} g(a)\right)^{[L:K]_i}$. We have, keeping in mind Lemma 4.14,

$$x(a) = \frac{[L:K]_i}{n} \sum_{g \in G} x(g(a)) = \frac{1}{n} x(N_{L/K}(a)) = \frac{1}{n} v(N_{L/K}(a)).$$

The last result follows directly. \square

Lemma 5.8. *Let $(L, w) \supseteq (K, v)$ be a finite purely inseparable extension of valued fields. Then k_w/k_v is purely inseparable and we have $e(w/v) = e_w(w/v)$.*

Proof. It is obvious that k_w/k_v is purely inseparable. Proposition 5.6 together with Lemma 5.7 imply $e(w/v) = e_w(w/v)$. \square

6. NORMAL EXTENSIONS

We will first consider finite extensions of valued fields, and then take a limit.

6.1. Finite normal extensions. In this subsection we let $(M, x) \supseteq (K, v)$ be a finite normal extension of valued fields with $G = \text{Aut}_K(M)$. For simplicity, we put $x_i = x|_{K_i, x}$, $x_h = x|_{K_h, x}$, $x_v = x|_{K_v, x}$ and $x_s = x|_{M_{K, \text{sep}}}$.

Proposition 6.1. *One has $[K_{h, x} : K] = g_{M, v}$. Furthermore x is the unique extension of x_h to M and one has $e(x_h/v) = f(x_h/v) = 1$.*

Proof. Since the action of G on the set of valuations of M extending v is transitive (Proposition 5.6), we have $[K_{h, x} : K] = g_{M, v}$. The second statement also follows from the transitivity of the action.

We will show $f(x_h/v) = 1$. Let $a \in \mathcal{O}_{x_h}$, and pick $\alpha_a \in K_{h, x}$ satisfying $\alpha_a - a \in \mathfrak{m}_{x_h}$ and α_a in the maximal ideal of any other valuation extending v to $K_{h, x}$ (Corollary 5.5). This means that for $\bar{g} \in G/D_{x, K}$ with $g \neq D_{x, K}$ we have $g(\alpha) \in \mathfrak{m}_{x_h}$. Then, by looking in M , one obtains

$$\text{tr}_{K_{h, x}/K}(\alpha_a) = \sum_{\bar{g} \in G/D_{x, K}} g(\alpha) \in a + \mathfrak{m}_{x_h}.$$

Notice that $\text{tr}_{K_{h, x}/K}(\alpha_a) \in K \cap \mathcal{O}_{x_h} = \mathcal{O}_v$. Hence the natural map $k_v \rightarrow k_{x_h}$ is surjective. This gives $f(x_h/v) = 1$.

Next we will prove $e(x_h/v) = 1$. Let $b \in K_{h, x}^*$. Take $m \in \mathbf{Z}$ such that for all $g \in G \setminus D_{x, K}$, we have $x_h(\alpha_1^m b) \neq x_h(g(\alpha_1^m b))$. To do this, one needs to make sure that for all $g \in G \setminus D_{x, K}$ one has $m(x(\alpha_1) - x(g(\alpha_1))) \neq x(g(b)) - x(b)$, which can easily be achieved since $x(\alpha_1) \neq x(g(\alpha_1))$, the group Δ_x is torsion-free and G is finite. Put $\beta = \alpha_1^m b$ and $f = \prod_{\bar{g} \in G/D_{x, K}} (X - \bar{g}(\beta)) = \sum_{i=0}^n a_i X^i \in K[X]$ with $a_n = 1$. Let $S = \{\bar{g}(\beta) : \bar{g} \in G/D_{x, K} \text{ s.t. } x_h(\bar{g}(\beta)) < x_h(\beta)\}$ and set $r = \#S$. Then one sees $x_h(a_{n-r}) = x_h(\prod_{c \in S} c)$ and $x_h(a_{n-r-1}) = x_h(\beta \prod_{c \in S} c)$. This gives $x_h(b) = x_h(\beta) = x_h(a_{n-r-1}/a_{n-r}) \in \Delta_v$ and we are done. \square

Proposition 6.2. *We have a short exact sequence*

$$0 \rightarrow I_{x,K} \rightarrow D_{x,K} \rightarrow \text{Aut}_{k_v}(k_x) \rightarrow 0$$

and k_x is normal over k_v . Furthermore we have $[K_{i,x} : K_{h,x}] = f(x_i/x_h) = f_s(x_i/x_h) = f_s(x/v)$ and $e(x_i/x_h) = 1$.

Proof. The exactness of the sequence and the normality of k_x over k_v follow from Corollary 4.13 and Proposition 5.4. We will now prove the last two statements. Look at the normal extension $M/K_{i,x}$ with group $I_{x,K}$. From the exact sequence for the extension $M/K_{i,x}$ just obtained we see that the zero map $I_{x,K} \rightarrow \text{Aut}_{k_{x_i}}(k_x)$ is surjective. We find $\text{Aut}_{k_{x_i}}(k_x) = 0$. As k_x/k_{x_i} is normal, this gives that k_x/k_{x_i} is purely inseparable. Consider the Galois extension $K_{i,x}/K_{h,x}$ with group $D_{x,K}/I_{x,K}$. We obtain an exact sequence

$$D_{x,K}/I_{x,K} \rightarrow \text{Aut}_{k_{x_h}}(k_{x_i}) = \text{Aut}_{k_v}(k_x) \rightarrow 0$$

(note that $k_v = k_{x_h}$ by Proposition 6.1). The first map is injective and hence we have an isomorphism. Using Proposition 5.6 we obtain:

$$\begin{aligned} e(x_i/x_h) \cdot f(x_i/x_h) &\leq [K_{i,x} : K_{h,x}] = \# \text{Aut}_{k_{x_h}}(k_{x_i}) \\ &= \# \text{Aut}_{k_v}(k_x) \leq [k_{x_i} : k_{x_h}] = f(x_i/x_h). \end{aligned}$$

Hence we find $[K_{i,x} : K_{h,x}] = f(x_i/x_h) = f_s(x_i/x_h) = f_s(x/v)$ and $e(x_i/x_h) = 1$. \square

Lemma 6.3. *Let $0 \rightarrow A \rightarrow B \xrightarrow{f} C \rightarrow 0$ be an exact sequence of abelian groups. Let H be the group of automorphisms of this sequence consisting of automorphisms which are the identity on C . Let $H' \subseteq H \subseteq \text{Aut}(B)$ the set of automorphisms which are the identity on A . Then the map*

$$\begin{aligned} \varphi: H &\rightarrow \text{Hom}(C, A) \rtimes \text{Aut}(A) \\ h &\mapsto (f(b) \mapsto h(b) - b, h|_A) \end{aligned}$$

is an injective morphism of groups. One has:

- i. $\varphi|_{H'}: H' \rightarrow \text{Hom}(C, A)$ is an isomorphism;
- ii. if $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is split, then φ is an isomorphism.

Proof. One easily shows that φ is well-defined and that it is a morphism of groups.

i: Consider the following map:

$$\begin{aligned} \psi: \text{Hom}(C, A) &\rightarrow H' \\ \sigma &\mapsto (b \in B \mapsto b + \sigma(f(b))) \end{aligned}$$

One then easily checks that this is the inverse of $\varphi|_{H'}$. This also shows that φ is injective.

ii: Consider the exact sequence $0 \rightarrow A \rightarrow A \oplus C \rightarrow C \rightarrow 0$. Consider the map

$$\begin{aligned} \chi: \text{Hom}(C, A) \rtimes \text{Aut}(A) &\rightarrow H \\ (\sigma, \tau) &\mapsto ((a, c) \mapsto (\sigma(c) + \tau(a), c)). \end{aligned}$$

One easily checks that both maps are inverse to each other. \square

We have an exact sequence $1 \rightarrow \mathcal{O}_x^*/(1 + \mathfrak{m}_x) \cong k_x^* \rightarrow M^*/(1 + \mathfrak{m}_x) \rightarrow \Delta_x \rightarrow 1$. Note that $D_{x,K}$ acts on such sequences and it acts on this sequence trivially on Δ_x (Lemma 4.15), it fixes $K^*/(1 + \mathfrak{m}_v)$ and the action on k_x^* comes from a field automorphism. Set $\Gamma_{x,v} = \text{im}(\text{Aut}_{k_v}(k_x) \rightarrow \text{Aut}_{k_v^*}(k_x^*))$. Let $\text{Aut}_{K^*, \Gamma_{x,v}}(M^*/(1 + \mathfrak{m}_x))$ be

the group of automorphisms of the sequence, seen as subgroup of $\text{Aut}(M^*/(1+\mathfrak{m}_x))$, which are the identity on $K^*/(1+\mathfrak{m}_x)$ and which induce an element of $\Gamma_{x,v}$ on k_x^* (note that the two conditions already imply that they act as the identity on Δ_x). We get a morphism $D_{x,K} \rightarrow \text{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x))$.

Note that the group $I_{x,K}$ acts trivially on k_x^* and $K^*/(1+\mathfrak{m}_v)$ and Δ_x . The automorphisms of the exact sequence with these properties correspond by Lemma 6.3 to $\text{Hom}(\Delta_x/\Delta_v, k_x^*)$ and this gives a morphism

$$\begin{aligned} I_{x,K} &\rightarrow \text{Hom}(\Delta_x/\Delta_v, k_x^*) \\ g &\mapsto \left(\bar{c} \mapsto \overline{g(c)/c} \right). \end{aligned}$$

By definition $V_{x,K}$ is the kernel of the last morphism.

Lemma 6.4. *Let $(L', u') \supseteq (L, u)$ be a finite normal extension of valued fields with group H . Assume that for all $a \in L'^*$ and $h \in H$ we have*

$$\frac{h(a)}{a} \in 1 + \mathfrak{m}_{u'}.$$

Then H is a p_u -group.

Proof. We can directly reduce to the case where L'/L is Galois and $[L' : L] > 1$. Let $a \in L'^*$ satisfy $\text{tr}_{L'/L}(a) = 0$, which exists by looking at dimensions. Then we have

$$0 = \frac{\text{tr}_{L'/L}(a)}{a} \in [L' : L] + \mathfrak{m}_{u'}.$$

This shows $\#H = [L' : L] = 0 \in k_u$ and hence H is a p_u -group. \square

Proposition 6.5. *The subgroup $V_{x,K}$ is the unique p_v -Sylow subgroup of $I_{x,K}$. The sequences*

$$0 \rightarrow V_{x,K} \rightarrow I_{x,K} \rightarrow \text{Hom}(\Delta_x/\Delta_v, k_x^*) \rightarrow 0$$

and

$$0 \rightarrow V_{x,K} \rightarrow D_{x,K} \rightarrow \text{Aut}_{K^*,\Gamma_{x,v}}(M^*/(1+\mathfrak{m}_x)) \rightarrow 0$$

are exact. One has $[K_{v,x} : K_{i,x}] = e(x_v/x_i) = e_t(x_v/x_i)$ and $f(x_v/x_i) = 1$. We also have $[M : K_{v,x}] \in p_v^{\mathbb{Z}_{\geq 0}}$ and $e(x/x_v) = e_w(x/x_v)$. Set $s = \text{ord}(I_{x,K}/V_{x,K})$. Then k_x has an s -th primitive root of unity.

Proof. Let $\varphi : I_{x,K} \rightarrow \text{Hom}(\Delta_x/\Delta_v, k_x^*)$ be the morphism with kernel $V_{x,K}$. Since k_x^* has no non-trivial elements of p_v -power order, all elements of order a power of p_v of $I_{x,K}$ are in $V_{x,K}$. Consider the normal extension $M/K_{v,x}$ with automorphism group $V_{x,K}$. One obtains that $V_{x,K}$ is a p_v -group by Lemma 6.4. Hence $V_{x,K}$ is the unique p_v -Sylow subgroup of $I_{x,K}$.

Consider the Galois extension $K_{v,x}/K_{i,x}$ with group $I_{x,K}/V_{x,K}$. As the order of $I_{x,K}/V_{x,K}$ is coprime with p_v , we have an exact sequence $0 \rightarrow I_{x,K}/V_{x,K} \rightarrow \text{Hom}(\Delta_{x_v}/\Delta_{x_i}, k_{x_v}^*)$. Using Proposition 5.6 we obtain

$$f(x_v/x_i) \cdot e(x_v/x_i) \leq [K_{v,x} : K_{i,x}] \leq \# \text{Hom}(\Delta_{x_v}/\Delta_{x_i}, k_{x_v}^*) \leq e_t(x_v/x_i) \leq e(x_v/x_i).$$

We obtain $f(x_v/x_i) = 1$ and $[K_{v,x} : K_{i,x}] = e(x_v/x_i) = e_t(x_v/x_i)$. We also obtain $\# \text{Hom}(\Delta_{x_v}/\Delta_{x_i}, k_{x_v}^*) = \#(I_{x,K}/V_{x,K})$. Finally we obtain that k_{x_v} has an s -th primitive root of unity.

One easily obtains $[M : K_{v,x}] \in \mathfrak{p}_v^{\mathbf{Z}_{\geq 0}}$. Furthermore, $e(x/x_v) = e_w(x/x_v)$ follows from Lemma 5.7.

The extension k_x/k_{x_v} is purely inseparable (Proposition 6.2). This shows that the torsion of k_x^* is equal to the torsion of $k_{x_v}^*$. Note that $\Delta_v = \Delta_{x_i}$ by Proposition 6.1 and Proposition 6.2. Hence we have a natural map $\text{Hom}(\Delta_x/\Delta_v, k_x^*) \rightarrow \text{Hom}(\Delta_{x_v}/\Delta_{x_i}, k_{x_v}^*)$. Because Δ_x/Δ_{x_v} is a \mathfrak{p}_v -group, this map is injective. We find $\#(I_{x,K} / V_{x,K}) \leq \# \text{Hom}(\Delta_x/\Delta_v, k_x^*) \leq \# \text{Hom}(\Delta_{x_v}/\Delta_{x_i}, k_{x_v}^*) = \#(I_{x,K} / V_{x,K})$.

This shows that the sequence $0 \rightarrow V_{x,K} \rightarrow I_{x,K} \rightarrow \text{Hom}(\Delta_x/\Delta_v, k_x^*) \rightarrow 0$ is exact.

We will show that the second sequence is exact. Recall that this sequence comes from the action of $D_{x,K}$ on $0 \rightarrow k_x^* \rightarrow M^*/(1 + \mathfrak{m}_x) \rightarrow \Delta_x \rightarrow 0$. If $\sigma \in D_{x,K}$ acts trivially on the exact sequence, then it acts trivially on k_x and hence lies in $I_{x,K}$ and hence in $V_{x,K}$. We will count $\text{Aut}_{K^*, \Gamma_{x,v}}(M^*/(1 + \mathfrak{m}_x))$. Note that the restriction map to $\text{Aut}_{K^*, \Gamma_{x,v}}(M^*/(1 + \mathfrak{m}_x)) \rightarrow \Gamma_{x,v}$, a group of cardinality $\# D_{x,K} / \# I_{x,K}$, is surjective (Proposition 6.2). Let $h \in \Gamma_{x,v}$. The set of automorphisms inducing h is in bijection with $\text{Hom}(\Delta_x/\Delta_v, k_x^*)$ (Lemma 6.3), and this set is of cardinality $\# I_{x,K} / \# V_{x,K}$. We find:

$$\# \text{Aut}_{K^*, \Gamma_{x,v}}(M^*/(1 + \mathfrak{m}_x)) = \# D_{x,K} / \# I_{x,K} \cdot \# I_{x,K} / \# V_{x,K} = \# D_{x,K} / \# V_{x,K}.$$

Hence the last sequence is exact. \square

We later use the following lemma, which summarizes part of the situation. In Proposition 3.7 we will give a more readable form.

Lemma 6.6. *Let $(M, x) \supseteq (K, v)$ be a finite normal extension of valued fields. Then the following statements hold:*

- i. $[K_{h,x} : K] = g_{M,v}$, $e(x_h/v) = f(x_h/v) = 1$;
- ii. $[K_{i,x} : K_{h,x}] = f_s(x_i/x_h) = f(x_i/x_h) = f_s(x/v)$, $e(x_i/x_h) = 1$;
- iii. $[K_{v,x} : K_{i,x}] = e_t(x_v/x_i) = e(x_v/x_i) = e_t(x/v)$, $f(x_v/x_i) = 1$;
- iv. $[M : K_{v,x}] \in \mathfrak{p}_v^{\mathbf{Z}_{\geq 0}}$, $e(x/x_v) = e_w(x/x_v) = e_w(x/v)$, $f(x/x_v) = f_i(x/x_v) = f_i(x/v)$.

Proof. This follows from combining Proposition 6.1, Proposition 6.2, Proposition 6.5 and Proposition 5.6. \square

6.2. Normal extensions.

Remark 6.7. Let $(M, x) \supseteq (K, v)$ be a normal extension of valued fields and let $G = \text{Aut}_K(M)$. Let \mathfrak{T} be the set of finite normal extensions of K in M . By definition one has

$$\begin{aligned} D_{x,K} &= \varprojlim_{M' \in \mathfrak{T}} D_{x|_{M'}, K}; \\ I_{x,K} &= \varprojlim_{M' \in \mathfrak{T}} I_{x|_{M'}, K}; \\ V_{x,K} &= \varprojlim_{M' \in \mathfrak{T}} V_{x|_{M'}, K}. \end{aligned}$$

All maps in the projective limits come from the natural restriction maps.

Lemma 6.8. *Let $K \subseteq L \subseteq M$ be algebraic extensions of fields. Then we have $M_{L,\text{sep}} = M_{K,\text{sep}}L$.*

Proof. Assume $p = \text{char}(K) \neq 0$. One obviously has $M_{L,\text{sep}} \supseteq M_{K,\text{sep}}L$. For $x \in M \setminus M_{K,\text{sep}}L$ there is $i \in \mathbf{Z}_{\geq 0}$ such that $x^{p^i} \in M_{K,\text{sep}}$, and hence $M/M_{K,\text{sep}}L$ is purely inseparable and we are done. \square

We need the following technical lemma.

Lemma 6.9. *Let $M \supseteq L \supseteq K$ be algebraic extensions of fields where M/K is normal. Let $G = \text{Aut}_K(M)$ and $H = \text{Aut}_L(M) \subseteq G$. Let $G' \subseteq G$ be a subgroup. Then one has $(M_{L,\text{sep}})^{G' \cap H} = (M_{K,\text{sep}})^{G'} L$.*

Proof. By Proposition 4.10 it is enough to show that both fields have the same compositum and intersection with $M_{K,\text{sep}}$. We start with the intersection, where we use Galois theory (for the first equality, note that $(M_{K,\text{sep}})^{G'} L / (M_{K,\text{sep}})^{G'} (L \cap M_{K,\text{sep}})$ is purely inseparable):

$$\begin{aligned} ((M_{K,\text{sep}})^{G'} L) \cap M_{K,\text{sep}} &= (M_{K,\text{sep}})^{G'} (L \cap M_{K,\text{sep}}) \\ &= (M_{K,\text{sep}})^{G'} (M_{K,\text{sep}})^H = (M_{K,\text{sep}})^{G' \cap H} \\ &= (M_{L,\text{sep}})^{G' \cap H} \cap M_{K,\text{sep}}. \end{aligned}$$

For the compositum, we have:

$$((M_{K,\text{sep}})^{G'} L) M_{K,\text{sep}} = M_{K,\text{sep}} L$$

and by Lemma 6.8 we have

$$LM_{K,\text{sep}} \subseteq (M_{L,\text{sep}})^{H \cap G'} M_{K,\text{sep}} \subseteq M_{L,\text{sep}} M_{K,\text{sep}} = LM_{K,\text{sep}}.$$

The result follows. \square

Proof of Theorem 3.6. We will first prove that the map $G \times S \rightarrow S$ is continuous. Take $x' \in S$, L a finite extension of K and suppose that $g \cdot x'' \in U_{x',L}$. Let N/K be a finite normal extension containing L in M . Then one has $\{g' \in G : g|_N = g'|_N\} \cdot U_{x'',N} \subseteq U_{x',L}$. This shows that the action is continuous. By definition the stabilizer of x is $D_{x,K}$ and this gives us the isomorphism $G/D_{x,K} \rightarrow S$.

One easily obtains for $g \in G$ the equalities $D_{g(x),K} = g D_{x,K} g^{-1}$ and $K_{h,g(x)} = g K_{h,x}$. The other cases are similar.

We want to show that the sequences are exact. The idea is that the result is a limit of the statements for finite normal extensions. This is the reason why the maps are morphisms of profinite groups. Let $0 \rightarrow A_i \rightarrow B_i \rightarrow C_i \rightarrow 0$ (i is some indexed set) be exact sequences of groups such that we can take a projective limit. Then the remaining sequence is left-exact. It is exact if all the maps $A_i \rightarrow A_j$ in the system are surjective (in this case, the so-called Mittag-Leffler condition is satisfied). See for example [AM69, Proposition 10.2] for a statement which is sufficient. Hence we take the limit of the sequences from Proposition 6.2 and Proposition 6.5.

Let M', M'' be finite normal over K with $K \subseteq M' \subseteq M'' \subseteq M$. We claim that the natural maps $I_{x|M'',K} \rightarrow I_{x|M',K}$ and $V_{x|M'',K} \rightarrow V_{x|M',K}$ are surjective. Take $g \in I_{x|M',K}$ with lift $g' \in \text{Aut}_K(M'')$. We have an exact sequence $0 \rightarrow I_{x|M'',M'} \rightarrow D_{x|M'',M'} \rightarrow \text{Aut}_{k_{x|M'}}(k_{x|M''}) \rightarrow 0$ from Proposition 6.2. This shows that there is a $g'' \in D_{x|M'',M'} \subseteq \text{Aut}_{M'}(M'')$ such that $g'g'' \in I_{x|M'',K}$ and $\overline{g'g''} = g \in \text{Aut}_K(M')$. A similar proof, using Proposition 6.5 and the result just obtained, shows the surjectivity of $V_{x|M'',K} \rightarrow V_{x|M',K}$.

This shows that all sequences in the limit remain exact (for the first one, we could have also used Corollary 4.13). Since $k_{x|M'}$ has enough roots of unity (Proposition 6.5) we find

$$\mathrm{Hom}(\Delta_x/\Delta_v, k_x^*) = \mathrm{Hom}(\lim_{\substack{\rightarrow \\ M'}} \Delta_{x|M'}/\Delta_v, k_x^*) = \lim_{\substack{\leftarrow \\ M'}} \mathrm{Hom}(\Delta_{x|M'}/\Delta_v, k_{x|M'}^*).$$

For the limit of the third sequence, we need to prove

$$\mathrm{Aut}_{K^*, \Gamma_{x,v}}(M^*/(1 + \mathfrak{m}_x)) = \lim_{\substack{\leftarrow \\ M'}} \mathrm{Aut}_{K^*, \Gamma_{x|M'}, v}(M^*/(1 + \mathfrak{m}_{x|M'}))$$

It is easy to see that the right group is contained in the left group. The other implication follows since such an automorphism of

$$1 \rightarrow k_x^* \rightarrow M^*/(1 + \mathfrak{m}_x) \rightarrow \Delta_x \rightarrow 1$$

induces an automorphism of

$$1 \rightarrow k_{x|M'}^* \rightarrow M'^*/(1 + \mathfrak{m}_{x|M'}) \rightarrow \Delta_{x|M'} \rightarrow 1$$

because $k_{x|M'}/k_v$ is normal (Proposition 6.2).

The statement about the pro- p_v -Sylow statement follow from Proposition 6.5. The normality of k_x/k_v follows from Proposition 6.2. Proposition 6.5 also gives the statement about the roots of unity.

Statement i directly follows from the definition. Statement ii follows from statement i and Lemma 6.9.

We will prove the exactness of the last three sequences. The only non-trivial part is the surjectivity of the last maps. The exactness for the last two sequences is as before, and the exactness of the first sequence follows from the transitivity of the action of G on S . The last statements then follow directly. \square

Lemma 6.10. *Suppose we have the following commutative diagram of groups with exact rows:*

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \xrightarrow{h} & C \longrightarrow 0 \\ & & \downarrow & & \downarrow f & & \downarrow g \\ 0 & \longrightarrow & A' & \longrightarrow & B' & \xrightarrow{h'} & C' \longrightarrow 0. \end{array}$$

Assume that $s: C \rightarrow B$ is a splitting of the first exact sequence and assume that $\mathrm{Hom}(\ker(g), A') = 0$. Then the map

$$\begin{aligned} s' : C' &\rightarrow B' \\ c' = g(c) &\mapsto f \circ s(c) \end{aligned}$$

is well-defined and it is a splitting of the second exact sequence.

Proof. Consider the morphism $f \circ s|_{\ker(g)}: \ker(g) \rightarrow B'$. Note that the image actually lands in A' and hence this is the 0 map. Hence s' is a well-defined map. Take $c'_1, c'_2 \in C'$, say with preimage c_1 respectively c_2 in C . Then $c_1 + c_2$ is a preimage of $c'_1 + c'_2$ and hence have

$$s'(c'_1 + c'_2) = f \circ s(c_1 + c_2) = f \circ s(c_1) + f \circ s(c_2) = s'(c'_1) + s'(c'_2).$$

This shows that s' is a morphism. For $c' \in C'$ with preimage $c \in C$ we find

$$h'(s'(c')) = h' \circ f \circ s(c) = g \circ h \circ s(c) = g(c) = c'.$$

\square

Proof of Theorem 3.8. We may assume that $K = K_{h,x}$. Set $\Gamma = \text{Aut}_{k_v}(\overline{k_x})$.

i: Let \overline{M} be an algebraic closure of M with valuation x' extending x . Let S be the set of intermediate fields L of $K_{v,x'}/K$ with the property that $(L, x'|_L) \supseteq (K, v)$ is totally ramified and tame. Order this set by inclusion. This set is not empty. Note that a chain has an upper bound, namely the union. By Zorn there is a maximal element, say L' . Notice that $\Delta_{x'}/\Delta_{x'|_{L'}}$ is a p_v -group. Indeed, if not, we could find a totally and tamely ramified extension of L' in \overline{M} by taking a root of an element of L' . Using the exact sequences (Theorem 3.6) it is not hard to see that $\text{Gal}(K_{v,x'}/L') \cong \Gamma$ (the extension $K_{v,x'}/L'$ has trivial V and hence trivial I). This shows that the sequence $0 \rightarrow I_{x',K}/V_{x',K} \rightarrow D_{x',K}/V_{x',K} \rightarrow \Gamma \rightarrow 0$ is split. We have the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & I_{x',K}/V_{x',K} & \longrightarrow & D_{x',K}/V_{x',K} & \longrightarrow & \Gamma \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & I_{x,K}/V_{x,K} & \longrightarrow & D_{x,K}/V_{x,K} & \longrightarrow & \text{Aut}_{k_v}(k_x) \longrightarrow 0. \end{array}$$

Lemma 6.10 gives us a splitting of the second sequence provided that we can show $\text{Hom}(\text{Aut}_{k_x}(\overline{k_x}), I_{x,K}/V_{x,K}) = 0$. Note that $I_{x,K}/V_{x,K} \cong \text{Hom}(\Delta_x/\Delta_v, k_x^*)$ (Theorem 3.6). Suppose we have such a non-trivial morphism. Then as Δ_x/Δ_v is torsion, we can find an element of prime order l coprime to p_v in Δ_x/Δ_v not mapping to zero (note that the order of l divides $\text{ord}(I_{x,K}/V_{x,K})$). This gives us a surjective morphism $\text{Aut}_{k_x}(\overline{k_x}) \rightarrow \mathbf{Z}/l\mathbf{Z}$. By assumption such a morphism does not exist.

ii: Note that $V_{x,K}$ is the unique pro- p_v -Sylow subgroup of $I_{x,K}$ (Theorem 3.6) and hence the statement trivially follows when $p_v = 1$ or when $p_v \nmid \text{ord}(I_{x,K})$. Assume $p_v \neq 1$ and $p_v \mid \text{ord}(I_{x,K})$. It is enough to show that the cohomological p_v -dimension of $D_{x,K}/V_{x,K}$, $\text{cd}_{p_v}(D_{x,K}/V_{x,K})$, is at most 1 [Ser02, Chapter I, Proposition 16]. We have an exact sequence $0 \rightarrow I_{x,K}/V_{x,K} \rightarrow D_{x,K}/V_{x,K} \rightarrow D_{x,K}/I_{x,K} \rightarrow 0$. From Theorem 3.6 it follows that $D_{x,K}/I_{x,K}$ is isomorphic to $\text{Aut}_{k_v}(k_x)$. This group has cohomological dimension at most 1 (see the proof of [Ser02, Chapter II, Proposition 3] or [Efr06, Theorem 22.2.1], in combination with Artin-Schreier theory). We have an isomorphism $I_{x,K}/V_{x,K} \cong \text{Hom}(\Delta_x/\Delta_v, k_x^*)$ and its order is coprime to p_v . Hence we have $\text{cd}_{p_v}(I_{x,K}/V_{x,K}) = 0$ ([Ser02, Chapter I, Corollary 2 on Page 19]). Using [Ser02, Chapter I, Proposition 15] we see that $\text{cd}_{p_v}(D_{x,K}/V_{x,K}) \leq 1$ and the result follows.

iii: This follows after combining i and ii and the fact that $V_{x,K}$ is a p_v -group (Theorem 3.6). \square

7. ALGEBRAIC EXTENSIONS

7.1. Proofs.

Proposition 7.1. *Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Let (M, x) be a finite normal extension of (K, v) containing (L, w) . Then the following hold:*

- i. *the quantity $n(w/v)$ is well-defined and one has $n(w/v) = \frac{g_{M,w}}{g_{M,v}} \cdot [L : K] = [L_{h,x} : K_{h,x}]$;*
- ii. *$d(w/v)$ is well-defined and has values in $p_v^{\mathbf{Z}_{\geq 0}}$.*

Furthermore, the quantities d , d_w , e , e_t , e_w , f , f_s , f_i and n are multiplicative in towers.

Proof. i. We will show that $n(w/v)$ is well-defined, i.e. does not depend on the choice of M . Let M' be another normal extension of K containing L with $G = \text{Aut}_K(M')$. Without loss of generality, we may assume $M' \supseteq M$. Put $H = \text{Aut}_M(M')$. Let X (respectively X') be the set of primes of M (respectively M') extending v . Note that G acts transitively on X' , and G/H acts transitively on X (Proposition 5.6). Then one easily shows that the map $X' \rightarrow X$ has equally sized fibers. Hence $g_{M',v} = \#X' = \#X \cdot \#(\text{fiber above } x) = g_{M,v} \cdot g_{M',x}$ as required. Similarly, if one replaces K by L , one obtains $g_{M',w} = g_{M,w} \cdot g_{M',x}$. Hence the required ratio does not depend on the choice of M .

From Lemma 6.6 and Theorem 3.6ii one obtains $[K_{h,x} : K] = g_{M,v}$ and $[LK_{h,x} : L] = [L_{h,x} : L] = g_{M,w}$. Hence we have

$$[L_{h,x} : K_{h,x}] = [LK_{h,x} : K_{h,x}] = \frac{[LK_{h,x} : L]}{[K_{h,x} : K]} \cdot [L : K] = \frac{g_{M,w}}{g_{M,v}} \cdot [L : K] = n(w/v).$$

We will now prove the last statement. It is obvious that e , e_t , e_w , f , f_s , f_i are multiplicative. If we show that n is multiplicative, it directly follows that d and d_w are multiplicative. Hence it is enough to show that n is multiplicative. Let (L', w') be a finite extension of (L, w) . Let M be a finite normal extension of K containing L' . Then one has

$$\begin{aligned} n(w'/w) n(w/v) &= \frac{g_{M,w'}}{g_{M,w}} \cdot [L' : L] \cdot \frac{g_{M,w}}{g_{M,v}} \cdot [L : K] \\ &= \frac{g_{M,w'}}{g_{M,v}} [L' : K] = n(w'/v). \end{aligned}$$

ii. It is now obvious that $d(w/v)$ is well-defined. One has $d(w/v) = \frac{[L_{h,x} : K_{h,x}]}{e(w/v)f(w/v)} \in \mathbf{Z}_{\geq 1}$ by Proposition 5.6, Proposition 6.1 and the multiplicativity of e and f .

If L/K is normal, one has

$$d(w/v) = \frac{[L : K_{h,w}]}{e(w/v)f(w/v)} = \frac{[L : K_{v,w}]}{e_w(w/v)f_s(w/v)} \in p_v^{\mathbf{Z}}$$

(Lemma 6.6). Together with the multiplicativity of d , this shows $d(w/v) \in p_v^{\mathbf{Z}_{\geq 0}}$ in general. \square

Proof of Proposition 3.7. This follows directly from Lemma 6.6 and the definitions. \square

Proof of Theorem 3.9. The first equality is easily from the definition, the second follows by definition and the third follows from Proposition 7.1ii. \square

Remark 7.2. Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields. Note that immediate implies unramified, unramified implies tame, totally wild implies totally ramified and totally ramified implies local.

Suppose that one of the following hold:

- i. w/v is immediate and local;
- ii. w/v is unramified and totally ramified;
- iii. w/v is tame and totally wild.

Then from Theorem 3.9 it follows that $L = K$.

Remark 7.3. Let $(L, w) \supseteq (K, v)$ be an algebraic extension of valued fields which is purely inseparable. Then one easily sees that it is totally wild (Lemma 5.8).

Proof of Theorem 3.10. The surjectivity of π follows directly from the transitivity as in Proposition 5.6 and the extension property as in Proposition 5.2.

Let $\sigma \in X$. This gives us embeddings $(K, v) \subseteq (L, w) \subseteq (M, x)$. Write $H = \text{Gal}(M/L)$. Then X corresponds to G/H . Let \mathfrak{T} be the set of finite normal subextensions of M/K . We first consider w/v :

i, ii, iii: w/v is immediate \iff for all $M' \in \mathfrak{T}$ the extension $w|_{M' \cap L}/v$ is immediate \iff for all $M' \in \mathfrak{T}$ we have $\# D_{x|_{M'}, K} = \# D_{x|_{M'}, L \cap M'}$ (Proposition 3.7, look at degrees such as $[K : K_{h, x|_{M'}}] = \# D_{x|_{M'}, K}$) \iff for all $M' \in \mathfrak{T}$ we have $D_{x|_{M'}, K} = D_{x|_{M'}, L \cap M'} = D_{x|_{M'}, K} \cap \text{Aut}_{L \cap M'}(M')$ (Theorem 3.6) \iff for all $M' \in \mathfrak{T}$ we have $D_{x|_{M'}, K} \subseteq \text{Aut}_{L \cap M'}(M')$ \iff $D_{x, K} \subseteq H$ (Theorem 3.6) \iff $L \subseteq K_{h, x}$. The other cases are similar.

iv, v, vi: w/v is local \iff for all $M' \in \mathfrak{T}$ the extension $w|_{M' \cap L}/v$ is local \iff for all $M' \in \mathfrak{T}$ we have $[L \cap M' : K][K_{h, x|_{M'}} : K] = [(L \cap M')_{h, x|_{M'}} : K_{h, x|_{M'}}][K_{h, x|_{M'}} : K] = [(L \cap M')K_{h, x|_{M'}} : K]$ (Proposition 3.7 and Theorem 3.6) \iff for all $M' \in \mathfrak{T}$ we have $\text{Aut}_K(M') = D_{x|_{M'}, K} \text{Aut}_{L \cap M'}(M')$ (as $K_{h, x}$ is separable, one can apply Proposition 4.2) \iff for all $M' \in \mathfrak{T}$ the group $D_{x|_{M'}, K}$ acts transitively on $\text{Aut}_K(M')/\text{Aut}_{L \cap M'}(M')$.

We prove that the last statement is equivalent with $D_{x, K}$ acting transitively on G/H . If $D_{x, K}$ acts transitively on G/H , then one easily sees from the surjectivity $G/H \rightarrow \text{Aut}_K(M')/\text{Aut}_{L \cap M'}(M')$ for $M' \in \mathfrak{T}$ and Theorem 3.6, that $D_{x|_{M'}, K}$ acts transitively on $\text{Aut}_K(M')/\text{Aut}_{L \cap M'}(M')$. Conversely, given $u, v \in G/H$, consider the projective system of non-empty finite sets which at level M' consists of those elements mapping $u|_{M'}$ to $v|_{M'}$. One can easily show that this set is non-empty and deduce the result. The other cases are similar.

Now consider x/w :

vii, viii, ix: x/w is immediate \iff $M \subseteq L_{h, x} = LK_{h, x}$ (using i and Theorem 3.6) \iff $M = LK_{h, x}$. The latter is equivalent to $[\sigma(L) : K]_i = [M : K]_i$ and $G_\sigma \cap D_{x, K} = 0$ by Galois theory. The proofs of viii and ix are similar.

x, xi, xii: x/w is local \iff M and $L_{h, x} = LK_{h, x}$ are linearly disjoint over L (using ii and Theorem 3.6) \iff $K_{h, x} \subseteq L$ iff $G_\sigma \subseteq D_{x, K}$. The proofs of xi and xii are similar.

Consider the last statements.

xiii: This follows from i and the surjectivity of π .

xiv: w is totally split in M \iff $M/\sigma(L)$ is separable and for all $g \in G$ we have $G_\sigma \cap D_{g(x), K} = 0$ (vii and Theorem 3.6) iff M/L is separable and only the trivial element of G_σ is conjugate to $D_{x, K}$ (Theorem 3.6). \square

Proof of Corollary 3.11. Let (E, x') be a normal extension of (K, v) extending the valued field (LL', x) .

i, ii, iii, iv: Assume that w/v is immediate. Theorem 3.10 gives us that $L \subseteq K_{h, x'}$. But then we have $LL' \subseteq L'K_{h, x'} = L'_{h, x'}$ (Theorem 3.6). Hence Theorem 3.10 shows that x/w' is immediate. The proofs for the other cases are similar. \square

Remark 7.4. Statements as in Corollary 3.11 are false for local, totally ramified or totally wild extensions. Here is an example from algebraic number theory. Let $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{7})$ and $L' = \mathbf{Q}(\sqrt{-1})$ and look at the primes above 2. In this case L/K and L'/K is totally wild (and hence local and totally ramified).

In the extension $L'' = \mathbf{Q}(\sqrt{-7})$ of \mathbf{Q} the prime 2 splits. Hence in the extension $LL'/K = \mathbf{Q}(\sqrt{7}, \sqrt{-1})/\mathbf{Q}(\sqrt{-1})$ the prime above 2 splits. The extension LL'/K is not local.

Proof of Corollary 3.12. Let (M, x) be a normal extension of (K, v) containing (L, w) .

For the immediate case, we have the following: $L \subseteq K_{h,x} \iff K' \subseteq K_{h,x}$ and $L \subseteq K'_{h,x} = K'K_{h,x}$ (Theorem 3.6). The result follows from Theorem 3.10. The unramified and tame cases are similar.

Now consider the local case. One has: $L \otimes_K K_{h,x}$ is a domain $\iff L \otimes_{K'} K'_{h,x}$ and $K' \otimes_K K_{h,x}$ are domains. Assume first that $K' \otimes_K K_{h,x}$ is a domain. Observe that

$$\begin{aligned} L \otimes_{K'} K'_{h,x} &= L \otimes_{K'} (K'K_{h,x}) \\ &= L \otimes_{K'} K' \otimes_K K_{h,x} \\ &= L \otimes_K K_{h,x} \end{aligned}$$

(Theorem 3.6). This directly proves \Leftarrow . The implication \Rightarrow follows from $K' \otimes_K K_{h,x} \subseteq L \otimes_K K_{h,x}$ and the above observation.

The result follows from Theorem 3.10. The totally ramified and totally wild cases are similar. \square

Proof of Corollary 3.15. Pick an extension $(M, x) \supseteq (L, w) \supseteq (K, v)$ such that M/K is normal. Using Theorem 3.10 we see $L_1 = K_{h,x} \cap L$, $L_2 = K_{i,x} \cap L$ and $L_3 = K_{v,x} \cap L$.

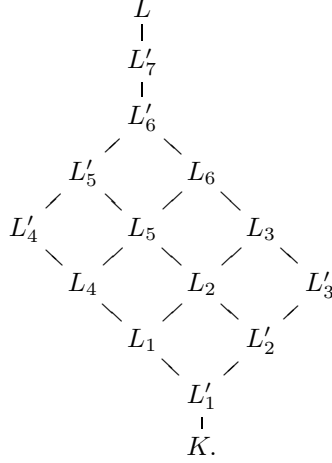
We will now construct a minimal local subextension. Assume that L' is a field such that $w/w|_{L'}$ is local. Then $w/w|_{L'_{K,\text{sep}}}$ is also local (Lemma 5.8). Hence we can replace L by $L_{K,\text{sep}}$. Using Theorem 3.10 and Theorem 3.6, we see that we need to find the smallest intermediate field L' of $L_{K,\text{sep}}/K$ such that $L_{K,\text{sep}}$ and $L'_{h,x} = L'K_{h,x}$ are linearly disjoint over L' . Such a field exists by Theorem 3.13 and it is denoted by $L_{K,\text{sep}} \setminus K_{h,x}$. The proofs of the other cases are similar when D is replaced by I respectively V .

We will now prove that $L_1 \subseteq L_4$. As $w|_{L_1}/v$ is immediate, it follows that the extension $w|_{L_1 L_4}/w|_{L_4}$ is immediate (Corollary 3.11). Hence $L_1 L_4/L_4$ is immediate and local. From Remark 7.2 it follows that $L_1 L_4 = L_4$, that is, $L_1 \subseteq L_4$. The inclusions $L_2 \subseteq L_5$ and $L_3 \subseteq L_6$ follow in a similar manner.

Assume that $g_{M,w} = 1$ for some normal extension M/K containing L . Note that $g_{M,w} = 1$ is equivalent to $H = \text{Aut}_L(M) \subseteq D_{x,K}$ (Theorem 3.10x). From Theorem 3.10 it follows that we need to show that $D_{x,K} \rightarrow \langle H, D_{x,K} \rangle / H$, $I_{x,K} \rightarrow \langle H, I_{x,K} \rangle / H$ and $V_{x,K} \rightarrow \langle H, V_{x,K} \rangle / H$ are surjective. The surjectivity of the first map is obvious, and the surjectivity of the second and third map is implied by the normality of $I_{x,K}$ respectively $V_{x,K}$ in $D_{x,K}$ (Theorem 3.6). \square

Actually, one can make the diagram a bit bigger. For $i = 1, 2, 3$ we define L'_i to be the intersection of the L_i while varying over the extensions of v to L . Similarly, for $i = 4, 5, 6$ we define L'_i to be the compositum of the L_i while varying over the extensions of v to L . For example, L'_1 is the maximal extension such that v is

totally split. If we put $L'_7 = L_{K,\text{sep}}$, we get the following diagram,



Proof of Corollary 3.16. We will prove ii. The other proofs are similar.

Assume that $g_{M,w} = 1$. Assume that w/v is not totally ramified. Then one has $L_2 = L_5$ in Corollary 3.15. And hence there is a non-trivial unramified extension in L/K . But then $L_5 L'/L'$ is unramified and non-trivial (Corollary 3.11 respectively $L \cap L' = K$). Contradiction. \square

Example 7.5. In Corollary 3.16 it is not enough to require that $L \cap L' = K$. Here is an example where all three statements are false. Consider the extension $L = \mathbf{Q}(\alpha)$ of \mathbf{Q} where α is a root of $x(x-1)^2 + 2$. Well-known techniques show that there are two primes above (2), namely $\mathfrak{p} = (2, \alpha)$ and $\mathfrak{q} = (2, \alpha - 1)$. One has $(2) = \mathfrak{p}\mathfrak{q}^2$. It follows that $\mathbf{Q}(\alpha)/\mathbf{Q}$ is not Galois. Hence the Galois closure M of this extension has group S_3 . Let $\bar{\alpha}$ be another root in this Galois closure and let $L' = \mathbf{Q}(\bar{\alpha})$. Then the prime (2) has the same splitting behavior in L'/\mathbf{Q} as in L/\mathbf{Q} , say $(2) = \mathfrak{p}'\mathfrak{q}'^2$. Note that $LL' = M$, $L \cap L' = \mathbf{Q}$. Furthermore, we know the splitting behavior of (2) in M : $(2) = \mathfrak{p}_1^2 \mathfrak{p}_2^2 \mathfrak{p}_3^2$ where there is just one prime above \mathfrak{p} respectively \mathfrak{p}' , which is totally wild, and there are two primes above \mathfrak{q} respectively \mathfrak{q}' . Say that \mathfrak{p}_1 lies above \mathfrak{p}' . Then $\mathfrak{p}_1/\mathfrak{p}'$ is totally wild, but $\mathfrak{p}_1|_{L/2\mathbf{Z}}$ is not even local. Hence statements i, ii and iii of Corollary 3.16 do not hold in this case.

The same example shows that in Corollary 3.15 it is not necessarily true that $L_1 = L_4$, $L_2 = L_5$ or $L_3 = L_6$. Indeed, for the extension $(\mathbf{Q}(\alpha), \mathfrak{q})/(\mathbf{Q}, 2\mathbf{Z})$ we have $L_1 = L_2 = L_3 = \mathbf{Q}$ and $L_4 = L_5 = L_6 = \mathbf{Q}(\alpha)$.

Example 7.6. Let K be a field with field extensions L, L' inside a field M . Assume that $L \cap L' = K$ and that M/L' is purely inseparable. Then L/K is purely inseparable. Indeed, if $\text{char}(k) = p > 0$, then for $x \in L$ there is $n \in \mathbf{Z}_{\geq 1}$ with $x^{p^n} \in L \cap L' = K$.

This statement also follows from our general theory. Consider the trivial valuation on K , that is, K is the valuation ring. This valuation has a unique valuation to any algebraic field extension of K . Furthermore, M/L' is totally wild. Hence from Corollary 3.16 it follows that L/K is totally wild and the result follows.

Proposition 7.7. Let (K, v) be a valued field and let L be an algebraic extension of K . Let $(M, x) \supseteq (K, v)$ be a normal extension of valued fields with group $G =$

$\text{Aut}_K(L)$ such that the G -set $X_L = \text{Hom}_K(L, M)$ is not empty. Then for any intermediate extension L' of L/K we have the following commutative diagram, where the maps are the natural maps:

$$\begin{array}{ccc} G \times X_L & \longrightarrow & X_L \\ \downarrow & & \downarrow \\ G \times X_{L'} & \longrightarrow & X_{L'}. \end{array}$$

The map

$$\begin{aligned} \varphi: D_{x,K} \setminus X_L &\rightarrow \{w \text{ of } L \text{ extending } v\} \\ D_{x,K} \sigma &\mapsto w \text{ s.t. } \mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L)) \end{aligned}$$

is a bijection of sets. Furthermore, for $\sigma \in X_L$ we have the following bijections:

$$\begin{aligned} D_{x,K} \sigma &\rightarrow \text{Hom}_{K_{h,x}}(\sigma(L)_{h,x}, M) \\ t\sigma &\mapsto t|_{\sigma(L)_{h,x}}, \\ I_{x,K} \sigma &\rightarrow \text{Hom}_{K_{i,x}}(\sigma(L)_{i,x}, M) \\ t\sigma &\mapsto t|_{\sigma(L)_{i,x}}, \end{aligned}$$

and

$$\begin{aligned} V_{x,K} \sigma &\rightarrow \text{Hom}_{K_{v,x}}(\sigma(L)_{v,x}, M) \\ t\sigma &\mapsto t|_{\sigma(L)_{v,x}}. \end{aligned}$$

Proof. The commutativity of the diagram is obvious.

Define $\varphi': X_L \rightarrow \{w \text{ of } L \text{ extending } v\}$ by putting $\sigma \mapsto w$ s.t. $\mathcal{O}_w = \sigma^{-1}(\mathcal{O}_x \cap \sigma(L))$. One should think of φ' as mapping an embedding $L \subseteq M$ to the restriction of x to L . The surjectivity is part of Theorem 3.10. Suppose $\varphi'(s) = \varphi'(t)$. There exists $h \in G$ such that $ht = s$. But then by Proposition 5.6 there exists $g \in \text{Aut}_{s(L)}(M)$ with $gh(x) = x$, that is, $gh \in D_{x,s(L)} \subseteq D_{x,K}$. We have $ghs = ht = s$. It is obvious that $\varphi'(D_{x,K}s) = \varphi'(s)$. This shows that the map is a bijection.

We will show that the map $D_{x,K} \sigma \rightarrow \text{Hom}_{K_{h,x}}(\sigma(L)_{h,x}, M)$ is a bijection. The other cases are similar. Suppose we have $\tau \in \text{Hom}_{K_{h,x}}(\sigma(L)_{h,x}, M)$. Then we can extend it to a morphism $\tau' \in \text{Aut}_{K_{h,x}}(M) = D_{x,K}$ and $\tau' \mapsto \tau$. \square

Proof of Proposition 3.17. The first statement directly follows from Proposition 7.7. The last statements follows from Proposition 7.7 and Proposition 3.7 and the separability of L/K . \square

Proof of Corollary 3.18. From Proposition 3.17 one sees that the set of valuations with the given properties is in bijection with the set of orbits of X under $D_{x,K}$ such that the length of such an orbit is equal to the length of the orbit under $I_{x,K}$. And this easily translates to the required statement. \square

7.2. Finding extensions explicitly.

Proposition 7.8. *Let (K, v) be a valued field and let L/K be a finite extension. Pick $a \in L$ which is integral over \mathcal{O}_v with minimal polynomial $f \in \mathcal{O}_v[x]$. Suppose that $\bar{f} = \prod_{i=1}^m f_i^{n_i} \in \mathbf{k}_v[x]$ where the f_i are monic irreducible and pairwise distinct. Then the following hold:*

- i. for $i = 1, \dots, m$ there are pairwise distinct valuations w_i on L with $f(w_i/v) \geq \deg(f_i)$;
- ii. if \bar{f} is separable, then the w_i are all valuations extending v to L and one has $f(w_i/v) = \deg(f_i)$, $e(w_i/v) = d(w_i/v) = 1$.

Proof. Notice that $fK[x] \cap R[x] = fR[x]$ as f is monic. Statement i follows directly from Proposition 5.2 and Proposition 5.4. Statement ii follows from i and Theorem 3.9. \square

If the valuation in the above statement is discrete, one can say a bit more. See for example [Sti09, Theorem 3.3.7].

8. DEFECTS IN THE DISCRETE CASE

In this section we will give examples of defects and show that under certain circumstances, defects do not occur. This section is quite different from the other sections in this article, but we felt it was needed to show the reader that defects are not necessarily a defect of our theory.

We start with an example where there is a defect.

Example 8.1. Let $(L, w) \supseteq (K, v)$ be a finite purely inseparable extension of valued fields where v is discrete, that is, $\Delta_v \cong \mathbf{Z}$. Then one can have $d(w/v) > 1$. Let p be a prime number. Consider $\mathbf{F}_p(t) \subseteq \mathbf{F}_p((t))$ with the valuation w_0 on $\mathbf{F}_p((t))$ with $w_0(t) = 1$. Let v_0 be its restriction to $\mathbf{F}_p(t)$. Then we have $\Delta_{v_0} = \Delta_{w_0}$ and $k_{v_0} = k_{w_0}$. Let $s \in \mathbf{F}_p((t))$ be transcendental over $\mathbf{F}_p(t)$ (such s exist, because $\overline{\mathbf{F}_p(t)}$ is countable, and $\mathbf{F}_p((t))$ is uncountable) and consider $K = \mathbf{F}_p(t, s^p) \subseteq \mathbf{F}_p(t, s) = L$, with restricted valuations v respectively w . This is a purely inseparable extension of degree p with the property that $g_{L,v} = e(w/v) = f(w/v) = 1$. From Proposition 5.6 and Theorem 3.9 we conclude $d(w/v) = p$.

We will show that in certain cases, there is no defect. We use the following lemma.

Lemma 8.2. *Let k be a field and let A be a localization at a multiplicative set of a finitely generated k -algebra which is a domain. Put $K = Q(A)$ and let L/K be a finite extension of fields. Then the integral closure \bar{A} of A in L is finite as A -module.*

Proof. Assume first that A is finitely generated as k -algebra.

Notice that it is enough to prove the statement for a finite extension of L . Indeed, a finitely generated module over a noetherian ring is a noetherian module ([AM69, Proposition 6.5]), and hence all submodules are finitely generated.

Noether normalization, [Liu02, Proposition 2.1.9], tells us that A is finite over a polynomial ring $A' = k[x_1, \dots, x_n]$ with quotient field K' . We show that the integral closure of A' in L , which is \bar{A} , is a finite A' -module and hence a finite A -module. This reduces to the case where $A = k[x_1, \dots, x_n]$.

We will start enlarging L . First enlarge it such that L/K is normal. We can split L/K into a tower $L \supseteq L' \supseteq K$ where L'/K is purely inseparable and L/L' is separable. Hence we are reduced to proving the following two cases:

- i. L/K separable;
- ii. L/K purely inseparable and $A = k[x_1, \dots, x_n]$.

Assume that L/K is separable. Let y_1, \dots, y_m be a basis of L/K with $y_i \in \overline{A}$. Let y'_1, \dots, y'_m be a dual basis of L/K with respect to the trace. Then it follows that $Ay_1 \oplus \dots \oplus Ay_m \subseteq \overline{A} \subseteq Ay'_1 \oplus \dots \oplus Ay'_m$. Note that $Ay'_1 \oplus \dots \oplus Ay'_m$ is a finitely generated module over a noetherian ring, and hence a finite A -module. It follows that \overline{A} is a finite A -module.

Assume that L/K is purely inseparable and $A = k[x_1, \dots, x_n]$. Since L/K is finite, we see that L is contained in $L' = l(x_1^{-p^d}, \dots, x_n^{-p^d})$ for some $d \in \mathbf{Z}_{\geq 0}$ large enough and l a finite (purely inseparable) extension of k . Replace L by L' . Notice that $A' = l[x_1^{-p^d}, \dots, x_n^{-p^d}]$ is integral over A and it is integrally closed. Hence the integral closure of A in L is A' , and it is finite over A .

We will now treat the general case. Write $A = S^{-1}B$ where B is a finitely generated k -algebra and S a multiplicative set. From [AM69, Proposition 5.12] we obtain $\overline{A} = S^{-1}\overline{B}$. We have shown that B is a finite A -module and hence \overline{A} is a finite A -module. \square

Proposition 8.3. *Let $(L, w) \supseteq (K, v)$ be a finite extension of valued fields. Suppose one of the following hold:*

- i. L/K is separable and $\Delta_v \cong \mathbf{Z}$;
- ii. \mathcal{O}_v contains a field k , $\mathcal{O}_v \neq K$, K finitely generated over k , and $\text{trdeg}_k(K) = 1$.

Then we have $\Delta_v \cong \mathbf{Z}$ and $d(w/v) = 1$.

Proof. First we prove that in the second case we also have $\Delta_v \cong \mathbf{Z}$. Let $x \in \mathcal{O}_v$ transcendental over k . Then $\mathfrak{p} = k[x] \cap \mathfrak{m}_v$ is a prime ideal. If it is zero, then $\mathcal{O}_v \supseteq k(x)$ and since K is finite over $k(x)$, it follows that $\mathcal{O}_v = K$, contradiction. Hence $\mathcal{O}_v \cap k(x) = k[x]_{\mathfrak{p}}$ (this follows since we know all valuations on $k(x)$ which are trivial on k). Notice that $k[x]_{\mathfrak{p}}$ is a discrete valuation ring, and hence the same follows for \mathcal{O}_v (as e is finite). Replace \mathcal{O}_v by $k[x]_{\mathfrak{p}}$ and K by $k(x)$ in this case. We will show the statement about $d(w/v)$ for the bigger extension, and the result about $d(w/v)$ follows from multiplicativity.

Now we will consider both cases at once. Let \mathcal{O} be the integral closure of \mathcal{O}_v in L . Assume first that \mathcal{O} is a finitely generated \mathcal{O}_v -module. Then one easily sees that \mathcal{O} is a free \mathcal{O}_v -module of rank $[L : K]$, since \mathcal{O}_v is a discrete valuation ring. Consider $\mathcal{O}/\mathfrak{m}_v\mathcal{O}$, which is isomorphic to $\prod_{w|v} \mathcal{O}_w/\mathfrak{m}_v\mathcal{O}_w$ (Proposition 5.4, in combination with theorems on artinian rings from [AM69]). Notice that $\mathcal{O}_w/\mathfrak{m}_v\mathcal{O}_w$ is a vector space over k_v of dimension $e(w/v)f(w/v)$ and the result follows.

Hence we are finished if we can show that \mathcal{O} is finite over \mathcal{O}_v . In the first case, this follows directly from the trace pairing. In the second case, use Lemma 8.2. \square

We will finish this section by giving an example of a separable extension of valued fields which has a defect. We start with the following lemma, which goes back to [Sch77]. We follow a proof from [Ste88].

Lemma 8.4. *Let K be a field and $n \in \mathbf{Z}_{\geq 1}$ be an integer coprime with $\text{char } K$. Let w be the number of n -th roots of unity in K . Let L be the splitting field of $x^n - a \in K[x]$. Then one has: L/K is abelian iff $a^w \in K^n$.*

Proof. We may assume $a \neq 0$.

\implies : Fix $\alpha \in L$ with $\alpha^n = a$ and let ζ_n be an n -th root of unity. Let $\sigma \in G = \text{Gal}(L/K)$. Write $\sigma(\zeta_n) = \zeta_n^{k(\sigma)}$. For $\tau \in G$ one has

$$\frac{\tau\sigma(\alpha)}{\sigma(\alpha)} = \frac{\sigma\tau(\alpha)}{\sigma(\alpha)} = \sigma\left(\frac{\tau(\alpha)}{\alpha}\right) = \left(\frac{\tau(\alpha)}{\alpha}\right)^{k(\sigma)} = \frac{\tau(\alpha^{k(\sigma)})}{\alpha^{k(\sigma)}}.$$

Hence $\alpha^{k(\sigma)}/\sigma(\alpha)$ is fixed by τ and hence lies in K . Its n -th power is $a^{k(\sigma)-1} \in K^n$. Let r be the greatest common divisor of n and $k(\sigma) - 1$ for $\sigma \in G$. Then we have $a^r \in K^n$. As $\langle \zeta_n^{n/r} \rangle$ is the set of G -invariant n -th roots of unity, one has $r = w$.

\Leftarrow : Suppose $a^w = b^n$ for some $b \in K$. One has $K \subseteq L \subseteq L' = K(b^{1/w}, \zeta_{nw})$. Notice that L'/K is abelian and hence L/K is abelian. \square

Remark 8.5. Next we will give an example of a separable extension which has a defect. Let p be a prime and consider the field \mathbf{Q}_p with its standard p -adic valuation. It is well-known that this valuation has a unique extension to each algebraic extension (\mathbf{Q}_p is *henselian*). Let L be the maximal tamely ramified extension of \mathbf{Q}_p . Put $L' = L(\zeta_{p^i} : i \in \mathbf{Z}_{\geq 1})$. We claim that for any finite extension L''/L' we have $d(L''/L') = [L'' : L']$ (we do not specify the valuations, since they are unique). Indeed, from the construction one easily sees that $e = f = 1$ (the residue field of L is already algebraically closed, and the value group of L' is \mathbf{Q}) and as the extension is unique, the degree is equal to the defect. We will now find a non-trivial extension L''/L' . We claim that $\sqrt[p^2]{p} \notin L'$. Suppose $\sqrt[p^2]{p} \in L'$, then $L(\sqrt[p^2]{p})/L$ is an abelian Galois extension. Note that $\#\{x \in L : x^{p^2} = 1\} = p$, as $\mathbf{Q}_p(\zeta_{p^2})/\mathbf{Q}_p$ is wild. Lemma 8.4 gives us $p^p \in L^{p^2}$. But this means that L/\mathbf{Q}_p is not tame, contradiction. Hence we can take $L'' = L'(\sqrt[p^2]{p})$.

REFERENCES

- [AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.
- [Efr06] Ido Efrat. *Valuations, orderings, and Milnor K-theory*, volume 124 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2006.
- [End72] Otto Endler. *Valuation theory*. Springer-Verlag, New York, 1972. To the memory of Wolfgang Krull (26 August 1899–12 April 1971), Universitext.
- [EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.
- [Kuh] Franz-Viktor Kuhlman. *Book on Valuation Theory (in preparation)*. <http://math.usask.ca/~fvk/Fvkbook.htm>.
- [Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Ern , Oxford Science Publications.
- [RV99] Dinakar Ramakrishnan and Robert J. Valenza. *Fourier analysis on number fields*, volume 186 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1999.
- [Sch77] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arith.*, 32(3):245–274, 1977.
- [Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1979. Translated from the French by Marvin Jay Greenberg.
- [Ser02] Jean-Pierre Serre. *Galois cohomology*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002. Translated from French to English by Patrick Ion and revised by the author.
- [Ste88] Peter Stevenhagen. Class groups and governing fields. *University of California, Berkeley*, 1988. Phd thesis.

- [Sti09] Henning Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, second edition, 2009.

MATHEMATISCH INSTITUUT P.O. BOX 9512 2300 RA LEIDEN THE NETHERLANDS

E-mail address: `mkosters@math.leidenuniv.nl`

URL: `www.math.leidenuniv.nl/~mkosters`